专有网络VPC 使用教程

产品版本：ZStack 3.3.0

文档版本：V3.3.0

ZStack

版权声明

商标说明

ZStack商标和其他云轴商标均为上海云轴信息科技有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受上海云轴公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，上海云轴公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1 介绍

专有网络VPC（Virtual Private Cloud，以下简称VPC），是基于VPC路由器和VPC网络共同组成的自定义私有云网络环境，帮助企业用户构建一个逻辑隔离的私有云。

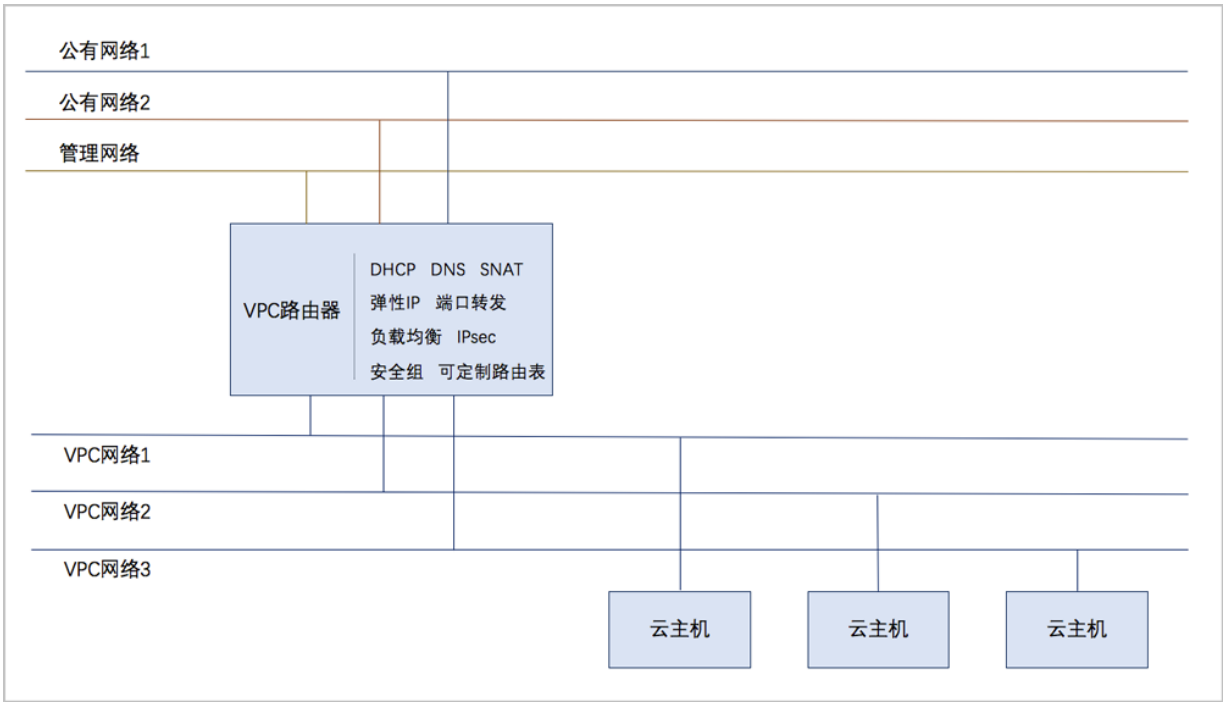
VPC路由器和VPC网络

VPC由VPC路由器和VPC网络组成。

1. VPC路由器：基于云路由规格直接创建的云路由器，拥有公有网络和管理网络。
   - VPC路由器是VPC的核心，可主动创建基于指定云路由规格的VPC路由器；
   - 须提前创建云路由规格所需的公有网络和管理网络、云路由镜像资源；
   - VPC路由器可灵活挂载或卸载VPC网络或其他公有网络；
   - 云路由规格定义的公有网络和管理网络，不可卸载；
   - 同一个云路由规格可以创建多个VPC路由器，这些VPC路由器共享使用同一个云路由规格里定义的公有网络段和管理网络段；
   - 公有网络作为默认网络，用于提供网络服务。
2. VPC网络：作为VPC的私有网络，可挂载至VPC路由器。
   - 须提前创建二层网络，用于创建三层的VPC网络；
   - 可在创建VPC网络时指定待挂载的路由器，也可创建VPC网络后再挂载路由器；
   - 如有云主机使用VPC网络，不支持从VPC路由器卸载；
   - 新建的网络段不可与VPC路由器内任一网络的网络段重叠。

VPC网络拓扑如图 *1: VPC网络拓扑示意图*所示：

图 1: VPC网络拓扑示意图



VPC特点

VPC具有以下特点：

- 灵活的网络配置，不同的VPC网络可灵活挂载到VPC路由器，每个VPC网络可自定义独立的网络段和独立的网关，VPC路由器支持加载/卸载网卡，并支持动态配置路由表和路由条目。
- 安全可靠的隔离，不同VPC下的VPC网络互相逻辑隔离，支持VLAN和VXLAN进行二层逻辑隔离，不同账户的VPC互不影响。
- 多子网互通：同一VPC下的多个VPC网络互联互通。
- 网络流量优化：支持分布式路由功能，优化东西向网络流量，并有效降低网络延迟。

VPC网络服务

VPC网络作为VPC的私有网络，使用VPC路由器提供各种网络服务。

- DHCP：默认采用扁平网络服务模块提供分布式DHCP服务。
- DNS：VPC路由器作为DNS服务器提供DNS服务。在云主机中看到的DNS地址默认为VPC路由器的IP地址，用户设置的DNS地址由VPC路由器负责转发配置。
- SNAT：VPC路由器向云主机提供原网络地址转换，云主机使用SNAT可直接访问外部互联网。
- 安全组：由安全组网络服务模块提供安全组服务，使用iptables进行云主机防火墙的安全控制。
- 弹性IP：可绑定弹性IP到VPC网络，实现公有网络到云主机私有网络的互联互通。
- 端口转发：提供公网IP到云主机私有网络IP的端口到端口的相关网络协议的互通。

- 负载均衡：将公网地址的访问流量分发到一组后端的云主机上，并自动检测并隔离不可用的云主机。
- IPsec隧道：使用IPsec隧道协议实现虚拟私有网络（VPN）的互联互通。

2 前提

在此教程中，假定已安装最新版本ZStack，并完成基本的初始化，包括区域、集群、物理机、镜像服务器、主存储等基本硬件资源的添加，以及计算规格的创建。具体方式请参考《用户手册》安装部署章节和Wizard引导设置章节。

本教程将详细介绍专有网络VPC的基本部署。

3 基本部署

背景信息

专有网络VPC的基本部署流程如下：

1. 创建二层公有网络，并加载此二层网络到相应集群。
2. 创建三层公有网络。
3. 创建二层管理网络，并加载此二层网络到相应集群。
4. 创建三层管理网络，用于与物理资源通信，例如，物理机、主存储、镜像服务器等。
5. 添加云路由镜像。
6. 创建云路由规格。
7. 基于云路由规格创建VPC路由器。
8. 创建二层私有网络（用于创建三层的VPC网络1），并加载此二层网络到相应集群。
9. 指定VPC路由器，创建三层的VPC网络1，注意网络段不可重叠。
10. 创建二层私有网络（用于创建三层的VPC网络2），并加载此二层网络到相应集群。
11. 指定VPC路由器，创建三层的VPC网络2，注意网络段不可重叠。
12. 使用VPC网络1创建云主机1，使用VPC网络2创建云主机2。
13. 验证VPC网络1与VPC网络2的互通性。

假定客户环境如下：

1. 公有网络

表 1: 公有网络配置信息

公有网络	配置信息
网卡	em01
VLAN ID	非VLAN
IP地址段	*10.108.10.100~10.108.10.200*
子网掩码	*255.0.0.0*
网关	*10.0.0.1*
DHCP IP	*10.108.10.101*

2. 管理网络

表 2: 管理网络配置信息

管理网络	配置信息
网卡	em02
VLAN ID	非VLAN
IP地址段	*192.168.29.10~192.168.29.20*
子网掩码	*255.255.255.0*
网关	*192.168.29.1*

注:

- 出于安全和稳定性考虑，建议部署独立的管理网络，并与公有网络隔离。
- 此管理网络与ZStack私有云中的管理网络为相同概念（即：管理物理机、主存储、镜像服务器的网络），如果已创建可直接复用。

3. VPC网络1

表 3: VPC网络1配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2800
IP CIDR	*192.168.10.0/24*
DHCP IP	*192.168.10.2*

4. VPC网络2

表 4: VPC网络2配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2900
IP CIDR	*192.168.11.0/24*
DHCP IP	*192.168.11.2*

以下介绍部署专有网络VPC的实践步骤。

操作步骤

1. 在ZStack私有云界面创建L2-公有网络。

   在ZStack私有云主菜单，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *1:* 公有网络配置信息填写如下：

   - **名称**：设置L2-公有网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2NoVlanNetwork
   - **网卡**：em01
   - **集群**：选择集群，如Cluster-1

   如图 *2:* 创建*L2-*公有网络所示，点击**确定**，创建L2-公有网络。

   图 2: 创建L2-公有网络

2. 在ZStack私有云界面创建L3-公有网络。

   在ZStack私有云主菜单，点击**网络资源** > **三层网络** > **公有网络**，进入**公有网络**界面，点击**创建公有网络**，在弹出的**创建公有网络**界面，参考上述表 *1:* 公有网络配置信息填写如下：

   - **名称**：设置L3-公有网络名称
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L2-公有网络
   - **关闭DHCP服务**：选择是否需要DHCP服务

   注:

   - 默认不勾选，表示启用DHCP服务，为云主机提供自动分配IP，此时DHCP IP支持自定义设置，也可由系统随机指定；

  - 勾选后，表示关闭DHCP服务，使用此网络的云主机将无法自动获取IP，需手动配置，此时DHCP IP不支持自定义设置，也不可由系统随机指定。

- **添加网络段**：选择IPv4类型网络地址、IP范围方式

  注: ZStack支持IPv4、IPv6类型网络地址；可通过IP范围或CIDR方式添加网络段。本教程以IPv4类型网络地址、IP范围方式为例。

- **起始IP**：*10.108.10.100*
- **结束IP**：*10.108.10.200*
- **子网掩码**：*255.0.0.0*
- **网关**：*10.0.0.1*
- **DHCP IP**：可选项，可按需设置DHCP IP

  注:

  - 若首次创建三层网络并启用DHCP服务，或对已启用DHCP服务的三层网络添加首个网络段，支持自定义设置DHCP IP；
  - 若三层网络已存在DHCP IP，添加网络段不允许自定义设置DHCP IP；
  - DHCP IP可以在添加的IP范围之内或之外，但必须在添加的IP范围所属的CIDR内，且未被占用；
  - 若留空不填，将由系统在添加的IP范围内随机指定。

- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *3: 创建L3-公有网络*所示，点击**确定**，创建L3-公有网络。

图 3: 创建L3-公有网络


确定
取消
创建公有网络
名称 *
L3-公有网络
简介
二层网络 *
L2-公有网络
关闭DHCP服务

3. 在ZStack私有云界面创建L2-管理网络。

   在ZStack私有云主菜单，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *2:* 管理网络配置信息填写如下：

   - **名称**：设置L2-管理网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2NoVlanNetwork

- **网卡**：em02
- **集群**：选择集群，如Cluster-1

如图 *4: 创建L2-管理网络*所示，点击**确定**，创建L2-管理网络。

图 4: 创建L2-管理网络

4. 在ZStack私有云界面创建L3-管理网络。

   在ZStack私有云主菜单，点击**网络资源** > **三层网络** > **系统网络**，进入**系统网络**界面，点击**创建系统网络**，在弹出的**创建系统网络**界面，参考上述*表 2: 管理网络配置信息*填写如下：

   - **名称**：设置L3-管理网络名称
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L2-管理网络

- **添加网络段**：选择IP范围
- **起始IP**：*192.168.29.10*
- **结束IP**：*192.168.29.20*
- **子网掩码**：*255.255.255.0*
- **网关**：*192.168.29.1*

如图 *5:* 创建*L3*-管理网络所示，点击**确定**，创建L3-管理网络。

图 5: 创建L3-管理网络

5. 添加云路由镜像。

   在ZStack私有云主菜单，点击 **网络资源** > **路由资源** > **云路由镜像**，进入**云路由镜像**界面，点击**添加云路由镜像**，在弹出的**添加云路由镜像**界面，可参考以下示例输入相应内容：

   - **名称**：设置云路由镜像名称
   - **简介**：可选项，可留空不填

- **镜像服务器**：选择待存放云路由镜像的镜像服务器，如BS-1
- **镜像路径**：支持添加URL路径或本地文件上传两种方式

1. **URL**：输入云路由镜像的可下载路径

   注:

   ZStack提供专用的云路由镜像供用户使用，可在*ZStack*官网下载最新的云路由镜像。

   - 文件名称：zstack-vrouter-3.3.0.qcow2
   - 下载地址：点击*ZStack*官网查看

2. **本地文件**：选择当前浏览器可访问的云路由镜像直接上传

   注:

   - 支持上传到镜像仓库和Ceph镜像服务器；
   - 采用本地浏览器作为中转上传镜像，请勿刷新或关闭当前浏览器，也不可停止管理节点服务，否则会添加失败。

如图 *6:* 添加云路由镜像所示，点击**确定**，添加云路由镜像。

图 6: 添加云路由镜像

6. 创建云路由规格。

在ZStack私有云主菜单，点击 **网络资源** > **路由资源** > **云路由规格**，进入**云路由规格**界面，点击**创建云路由规格**，在弹出的**创建云路由规格**界面，可参考以下示例输入相应内容：

- **名称**：设置云路由规格名称
- **简介**：可选项，可留空不填
- **CPU**：设置CPU个数，生产环境中建议个数设置为8以上
- **内存**：设置内存大小，单位包括：M、G、T，生产环境中建议设置为8G以上
- **镜像**：选择已添加的云路由镜像
- **管理网络**：从网络列表中选择已创建的L3-管理网络
- **公有网络**：从网络列表中选择已创建的L3-公有网络

如图 *7: 创建云路由规格*所示，点击**确定**，创建云路由规格。

图 7: 创建云路由规格

7. 基于云路由规格创建VPC路由器。

   在ZStack私有云主菜单，点击**网络资源** > **VPC** > **VPC路由器**，进入**VPC路由器**界面，点击**创建VPC路由器**，在弹出的**创建VPC路由器**界面，可参考以下示例输入相应内容：

   - **名称**：设置VPC云路由规格名称
   - **简介**：可选项，可留空不填
   - **云路由规格**：选择已创建的云路由规格

- **DNS**：可选项，用于设置VPC路由器的DNS解析服务，默认指定223.5.5.5

如图 *8: 创建VPC路由器*所示，点击**确定**，创建VPC路由器。

图 8: 创建VPC路由器

8. 在ZStack私有云界面创建L2-私有网络（用于创建三层的VPC网络1）。

在ZStack私有云主菜单，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *3: VPC网络1配置信息*填写如下：

- **名称**：设置L2-私有网络名称
- **简介**：可选项，可留空不填
- **类型**：选择L2VlanNetwork
- **Vlan ID**：2800
- **网卡**：em01
- **集群**：选择集群，如Cluster-1

如图 *9: 创建L2-私有网络*所示，点击**确定**，创建L2-私有网络。

图 9: 创建L2-私有网络

9. 指定VPC路由器，在ZStack私有云界面创建三层的VPC网络1。

   在ZStack私有云主菜单，点击**网络资源** > **VPC** > **VPC网络**，进入**VPC网络**界面，点击**创建VPC网络**，在弹出的**创建VPC网络**界面，参考上述*表 3: VPC网络1配置信息*填写如下：

   - **名称**：设置VPC网络1名称
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L2-私有网络
   - **关闭DHCP服务**：选择是否需要DHCP服务

注:

- 默认不勾选，表示启用DHCP服务，为云主机提供自动分配IP，此时DHCP IP支持自定义设置，也可由系统随机指定；
- 勾选后，表示关闭DHCP服务，使用此网络的云主机将无法自动获取IP，需手动配置，此时DHCP IP不支持自定义设置，也不可由系统随机指定。

- **VPC路由器**：可选项，VPC路由器可在创建VPC网络时指定，也可在创建VPC网络后再挂载
- **添加网络段**：选择CIDR
- **CIDR**：*192.168.10.0/24*

注: 网络段不可重叠。

- **DHCP IP**：可选项，可按需设置DHCP IP

注:

- 若首次创建三层网络并启用DHCP服务，或对已启用DHCP服务的三层网络添加首个网络段，支持自定义设置DHCP IP；
- 若三层网络已存在DHCP IP，添加网络段不允许自定义设置DHCP IP；
- DHCP IP必须在添加的CIDR内，且未被占用；
- 若留空不填，将由系统在添加的CIDR内随机指定；
- CIDR内首个IP地址已被默认为网关，不可作为DHCP IP。

如图 *10: 创建VPC网络1*所示，点击**确定**，创建VPC网络1。

图 10: 创建VPC网络1

10.在ZStack私有云界面创建L2-私有网络（用于创建三层的VPC网络2）。

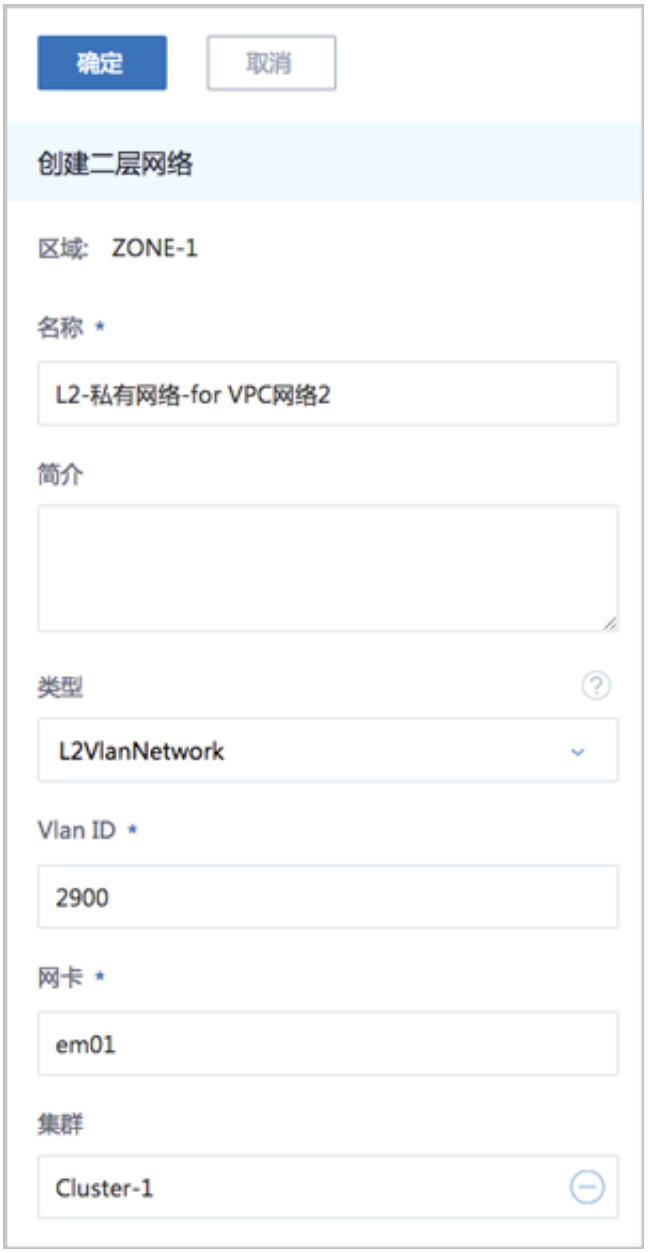
在ZStack私有云主菜单，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *4: VPC网络2配置信息*填写如下：

- **名称**：设置L2-私有网络名称
- **简介**：可选项，可留空不填

- **类型**：选择L2VlanNetwork
- **Vlan ID**：2900
- **网卡**：em01
- **集群**：选择集群，如Cluster-1

如图 *11: 创建L2-私有网络*所示，点击**确定**，创建L2-私有网络。

图 11: 创建L2-私有网络



11.指定VPC路由器，在ZStack私有云界面创建三层的VPC网络2。

在ZStack私有云主菜单，点击**网络资源** > **VPC** > **VPC网络**，进入**VPC网络**界面，点击**创建VPC网络**，在弹出的**创建VPC网络**界面，参考上述表 *4: VPC网络2配置信息*填写如下：

- **名称**：设置VPC网络2名称
- **简介**：可选项，可留空不填
- **二层网络**：选择已创建的L2-私有网络
- **VPC路由器**：可选项，VPC路由器可在创建VPC网络时指定，也可在创建VPC网络后再挂载
- **关闭DHCP服务**：选择是否需要DHCP服务

  注:

  - 默认不勾选，表示启用DHCP服务，为云主机提供自动分配IP，此时DHCP IP支持自定义设置，也可由系统随机指定；
  - 勾选后，表示关闭DHCP服务，使用此网络的云主机将无法自动获取IP，需手动配置，此时DHCP IP不支持自定义设置，也不可由系统随机指定。
- **添加网络段**：选择CIDR
- **CIDR**：*192.168.11.0/24*

  注: 网络段不可重叠。
- **DHCP IP**：可选项，可按需设置DHCP IP

  注:

  - 若首次创建三层网络并启用DHCP服务，或对已启用DHCP服务的三层网络添加首个网络段，支持自定义设置DHCP IP；
  - 若三层网络已存在DHCP IP，添加网络段不允许自定义设置DHCP IP；
  - DHCP IP必须在添加的CIDR内，且未被占用；
  - 若留空不填，将由系统在添加的CIDR内随机指定；
  - CIDR内首个IP地址已被默认为网关，不可作为DHCP IP。

如图 *12: 创建VPC网络2*所示，点击**确定**，创建VPC网络2。

图 12: 创建VPC网络2

12.使用VPC网络1创建私有云云主机1，使用VPC网络2创建私有云云主机2。

a) 使用VPC网络1创建私有云云主机1。

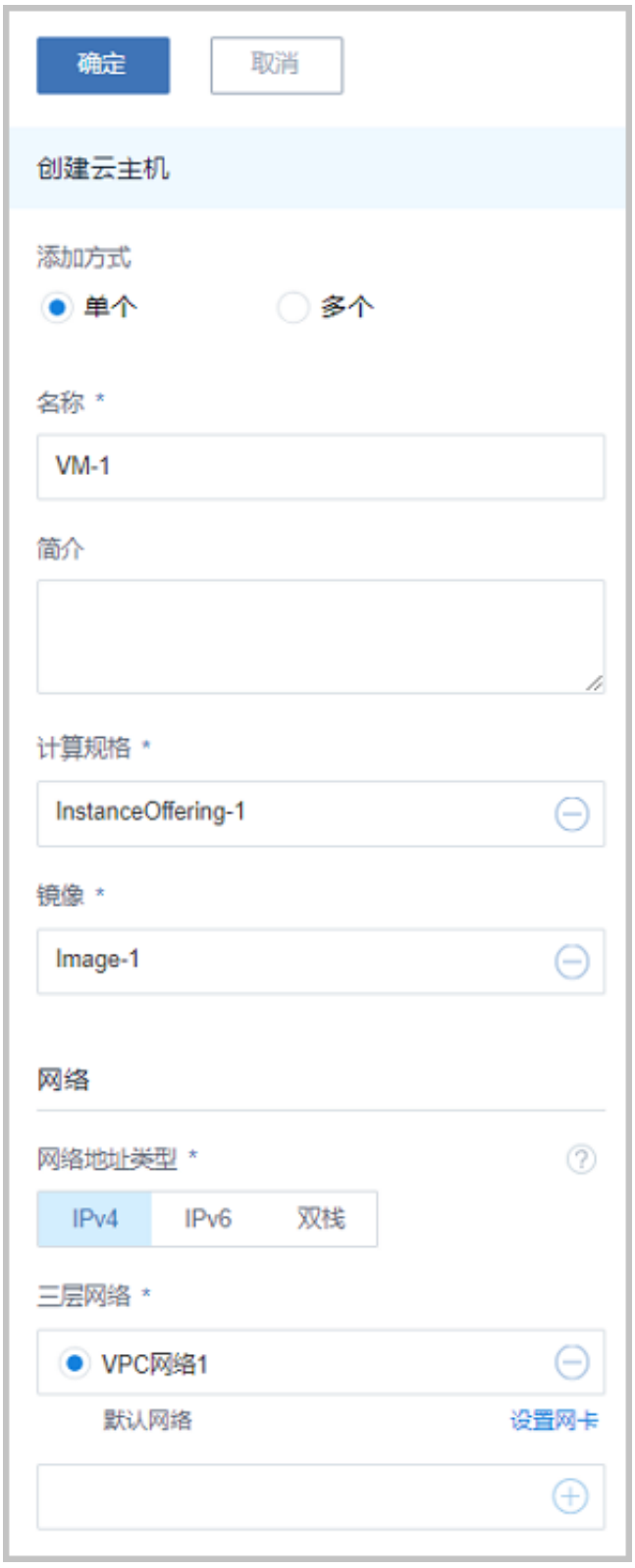
在ZStack私有云主菜单，点击 **云资源池** > **云主机**，进入**云主机**界面，点击**创建云主机**，在弹出的**创建云主机**界面，可参考以下示例输入相应内容：

- **添加方式**：单个

- **名称**：设置私有云云主机1名称，例如VM-1
- **简介**：可选项，可留空不填
- **计算规格**：选择已创建的计算规格
- **镜像**：选择已添加的云主机镜像
- **网络**：选择IPv4网络地址类型中的VPC网络1

如图 *13:* 创建私有云云主机*1*所示，点击 **确定**，创建私有云云主机1。

图 13: 创建私有云云主机1

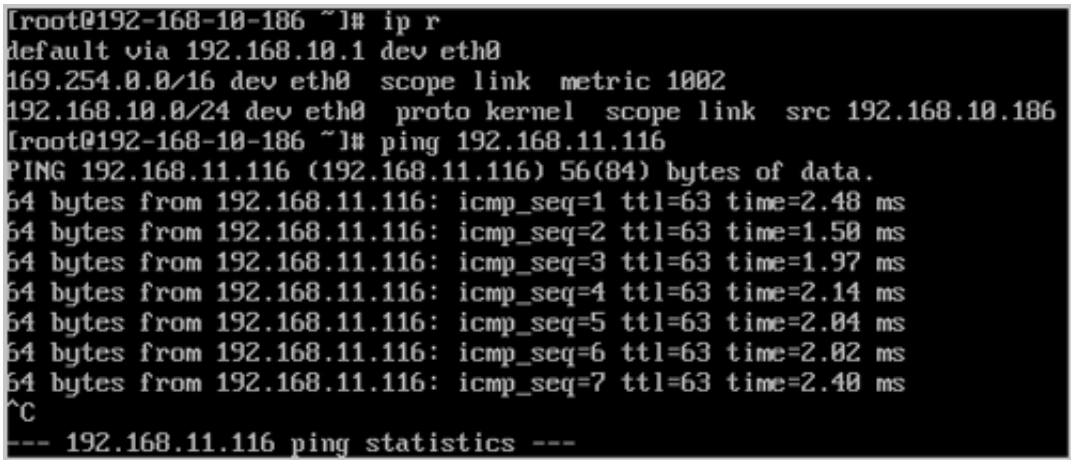


b) 同理，使用VPC网络2创建私有云云主机2。

13.验证VPC网络1与VPC网络2的互通性。

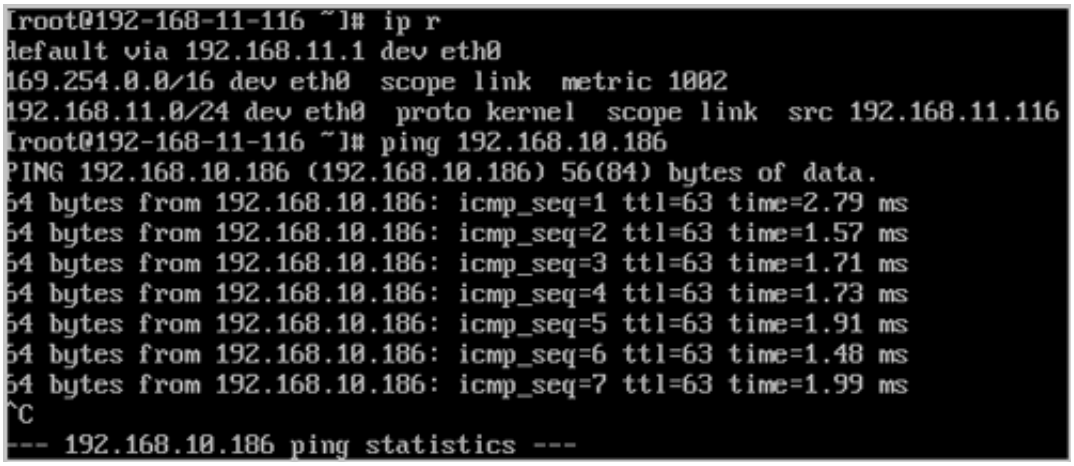
1. 登录VM-1，检查是否能够ping通VM-2，如图 *14: VM-1 ping通 VM-2*所示：

图 14: VM-1 ping通 VM-2



2. 登录VM-2，检查是否能够ping通VM-1，如图 *15: VM-2 ping通 VM-1*所示：

图 15: VM-2 ping通 VM-1



后续操作

至此，专有网络VPC的基本部署实践介绍完毕。

4 应用场景

专有网络VPC可用于以下典型应用场景：

- 多租户隔离
- 多层Web服务器
- 安全组
- 弹性IP
- 端口转发
- 负载均衡
- IPsec隧道

4.1 多租户隔离

前提条件

使用VLAN或VXLAN技术，可提供多租户在二层网络上的隔离。

表 5: VLAN与VXLAN的比较

VLAN	VXLAN
• VLAN最多支持4096个VLan ID，即一套环境中最多提供4096个隔离的租户网络，难以满足大规模云计算数据中心的需求 • 各厂商交换机配置VLAN方式各不相同	• VXLAN基于客户机房现有的网络拓扑，提供16M个逻辑网络用于多租户隔离 • VXLAN是基于现有三层网络之上Overlay虚拟出的二层网络，该Overlay虚拟过程可由软件方式实现，也可由支持VXLAN的交换机实现，客户可按需选择 • 相较于VLAN，VXLAN性能损耗较大，网络延迟也较高

背景信息

本场景主要介绍VXLAN-VPC网络提供多租户隔离的实践。

搭建多租户隔离VXLAN-VPC网络的基本流程：

1. 在admin账户下创建两个普通账户，账户A和账户B。
2. 在admin账户下创建二层公有网络，并加载此二层网络到相应集群。
3. 在admin账户下创建三层公有网络。
4. 在admin账户下创建二层管理网络，并加载此二层网络到相应集群。

5. 在admin账户下创建三层管理网络，用于与物理资源通信，例如，物理机、主存储、镜像服务器等。
6. 在admin账户下添加云路由镜像。
7. 在admin账户下创建云路由规格，并共享给账户A和账户B。
8. 在admin账户下创建VXLAN网络池，加载到相应集群，并共享给账户A和账户B。
9. 基于云路由规格在账户A和账户B分别创建一个VPC路由器。例如：VPC路由器-A和VPC路由器-B。
10. 基于VXLAN网络池在账户A和账户B分别创建两个VXLAN网络（虚拟的二层网络），例如：L2-VXLAN-A1和L2-VXLAN-A2、L2-VXLAN-B1和L2-VXLAN-B2。
11. 使用四个VXLAN网络分别在各自账户创建VPC网路，例如：VPC网络-A1和VPC网络-A2、VPC网络-B1和VPC网络-B2。
12. 使用四个VPC网络分别在各自账户创建一个云主机，例如：VM-A1、VM-A2、VM-B1和VM-B2。
13. 验证四台云主机之间的连通性。
14. 从admin账户共享三层公有网络给账户A和账户B。
15. 给VM-A1和VM-B1添加路由表。
16. 验证云主机VM-A1和VM-B1之间的连通性。

注:

- VXLAN网络池和VXLAN网络共同提供了VXLAN网络类型的配置；
- 使用VXLAN网络需先创建VXLAN网络池，VXLAN网络对应了VXLAN网络池里的一个虚拟网络；
- VXLAN网络池不能用于创建三层网络，只表示VXLAN网络的集合，VXLAN网络可用于创建三层网络。

假定客户环境如下：

1. 公有网络

表 6: 公有网络配置信息

公有网络	配置信息
网卡	em01
VLAN ID	非VLAN

公有网络	配置信息
IP地址段	*10.151.10.100~10.151.10.200*
子网掩码	*255.0.0.0*
网关	*10.0.0.1*
DHCP IP	*10.151.10.101*

2. 管理网络

表 7: 管理网络配置信息

管理网络	配置信息
网卡	em02
VLAN ID	非VLAN
IP地址段	*192.168.28.100~192.168.28.200*
子网掩码	*255.255.255.0*
网关	*192.168.28.1*

注:

- 出于安全和稳定性考虑，建议部署独立的管理网络，并与公有网络隔离。
- 此管理网络与ZStack私有云中的管理网络为相同概念（即：管理物理机、主存储、镜像服务器的网络），如果已创建可直接复用。

3. VXLAN网络池

表 8: VXLAN网络池配置信息

VXLAN网络池	配置信息
Vni范围	20-1200
VTEP CIDR	192.168.28.1/24

4. VPC网络-A1

表 9: VPC网络-A1配置信息

VPC网络	配置信息
网卡	em01

VPC网络	配置信息
IP CIDR	*192.168.21.0/24*

5. VPC网络-A2

表 10: VPC网络-A2配置信息

VPC网络	配置信息
网卡	em01
IP CIDR	*192.168.22.0/24*

6. VPC网络-B1

表 11: VPC网络-B1配置信息

VPC网络	配置信息
网卡	em01
IP CIDR	*192.168.23.0/24*

7. VPC网络-B2

表 12: VPC网络-B2配置信息

VPC网络	配置信息
网卡	em01
IP CIDR	*192.168.24.0/24*

以下介绍搭建VXLAN-VPC网络的实践步骤。

操作步骤

1. 在admin账户下创建两个普通账户，账户A和账户B。

   在ZStack私有云界面，点击**平台管理** > **用户管理** > **账户**按钮，在**账户**页面点击**创建账户**按钮，在**创建账户**窗口，可参考以下示例输入相应内容：

   - **名称**：设置账户名称，不区分大小写，例如：账户A
   - **简介**：可选项，可留空不填
   - **新密码**：设置登录该账户的密码
   - **确认密码**：重复输入密码，避免误输

如图 *16:* 创建账户所示，点击**确定**按钮，完成账户A创建。

图 16: 创建账户

同理，创建账户B，创建完成后如图 *17:* 账户创建完成所示：

图 17: 账户创建完成

2. 在admin账户下创建二层公有网络，并加载此二层网络到相应集群。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *6:* 公有网络配置信息填写如下：

   - **名称**：设置L2-公有网络名称

- **简介**：可选项，可留空不填
- **类型**：选择L2NoVlanNetwork
- **网卡**：em01
- **集群**：选择集群，如Cluster-1

如图 *18: 创建L2-公有网络*所示，点击**确定**，创建L2-公有网络。

图 18: 创建L2-公有网络

3. 在admin账户下创建三层公有网络。

   在ZStack私有云界面，点击**网络资源** > **三层网络** > **公有网络**，进入**公有网络**界面，点击**创建公有网络**，在弹出的**创建公有网络**界面，参考上述表 *6: 公有网络配置信息*填写如下：

- **名称**：设置L3-公有网络名称
- **简介**：可选项，可留空不填
- **二层网络**：选择已创建的L2-公有网络
- **关闭DHCP服务**：选择是否需要DHCP服务

  注:

  - 默认不勾选，表示启用DHCP服务，为云主机提供自动分配IP，此时DHCP IP支持自定义设置，也可由系统随机指定；
  - 勾选后，表示关闭DHCP服务，使用此网络的云主机将无法自动获取IP，需手动配置，此时DHCP IP不支持自定义设置，也不可由系统随机指定。
- **添加网络段**：选择IPv4类型网络地址、IP范围方式

  注: ZStack支持IPv4、IPv6类型网络地址；可通过IP范围或CIDR方式添加网络段。本教程以IPv4类型网络地址、IP范围方式为例。
- **起始IP**：*10.108.12.0*
- **结束IP**：*10.108.13.255*
- **子网掩码**：*255.0.0.0*
- **网关**：*10.0.0.1*
- **DHCP IP**：可选项，可按需设置DHCP IP

  注:

  - 若首次创建三层网络并启用DHCP服务，或对已启用DHCP服务的三层网络添加首个网络段，支持自定义设置DHCP IP；
  - 若三层网络已存在DHCP IP，添加网络段不允许自定义设置DHCP IP；
  - DHCP IP可以在添加的IP范围之内或之外，但必须在添加的IP范围所属的CIDR内，且未被占用；
  - 若留空不填，将由系统在添加的IP范围内随机指定。
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *19:* 创建*L3*-公有网络所示，点击**确定**，创建L3-公有网络。

图 19: 创建L3-公有网络

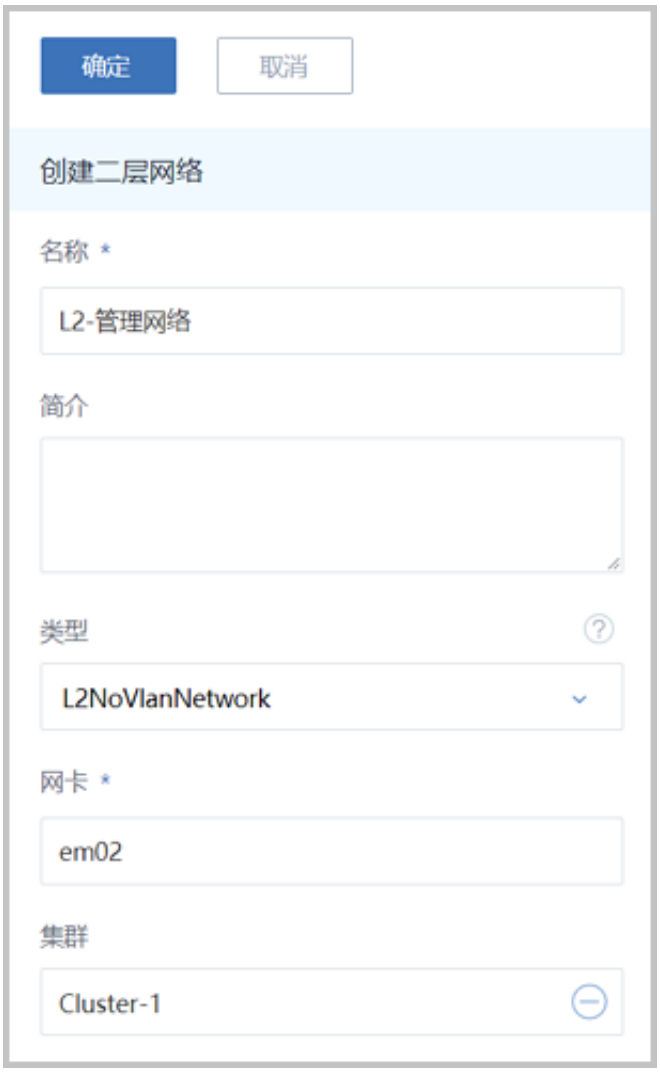
4. 在admin账户下创建二层管理网络，并加载此二层网络到相应集群。

在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *7:* 管理网络配置信息填写如下：

- **名称**：设置L2-管理网络名称
- **简介**：可选项，可留空不填
- **类型**：选择L2NoVlanNetwork
- **网卡**：em02
- **集群**：选择集群，如Cluster-1

如图 *20:* 创建*L2*-管理网络所示，点击**确定**，创建L2-管理网络。

图 20: 创建L2-管理网络



5. 在admin账户下创建三层管理网络，用于与物理资源通信，例如，物理机、主存储、镜像服务器等。

在ZStack私有云界面，点击**网络资源** > **三层网络** > **系统网络**，进入**系统网络**界面，点击**创建系统网络**，在弹出的**创建系统网络**界面，参考上述表 *7:* 管理网络配置信息填写如下：

- **名称**：设置L3-管理网络名称
- **简介**：可选项，可留空不填
- **二层网络**：选择已创建的L2-管理网络
- **添加网络段**：选择IP范围
- **起始IP**：*192.168.28.100*
- **结束IP**：*192.168.28.200*
- **子网掩码**：*255.255.255.0*
- **网关**：*192.168.28.1*

如图 *21:* 创建*L3*-管理网络所示，点击**确定**，创建L3-管理网络。

图 21: 创建L3-管理网络

6. 在admin账户下添加云路由镜像。

   在ZStack私有云主菜单，点击 **网络资源 > 路由资源 > 云路由镜像**，进入**云路由镜像**界面，点击**添加云路由镜像**，在弹出的**添加云路由镜像**界面，可参考以下示例输入相应内容：

   - **名称**：设置云路由镜像名称

- **简介**：可选项，可留空不填
- **镜像服务器**：选择待存放云路由镜像的镜像服务器，如BS-1
- **镜像路径**：支持添加URL路径或本地文件上传两种方式

  1. **URL**：输入云路由镜像的可下载路径

     注:

     ZStack提供专用的云路由镜像供用户使用，可在*ZStack*官网下载最新的云路由镜像。

     - 文件名称：zstack-vrouter-3.3.0.qcow2
     - 下载地址：点击*ZStack*官网查看

  2. **本地文件**：选择当前浏览器可访问的云路由镜像直接上传

     注:

     - 支持上传到镜像仓库和Ceph镜像服务器；
     - 采用本地浏览器作为中转上传镜像，请勿刷新或关闭当前浏览器，也不可停止管理节点服务，否则会添加失败。

7. 在admin账户下创建云路由规格，并共享给账户a和账户b。

   a) 在admin账户下创建云路由规格。

   在ZStack私有云主菜单，点击 **网络资源** > **路由资源** > **云路由规格**，进入**云路由规格**界面，点击**创建云路由规格**，在弹出的**创建云路由规格**界面，可参考以下示例输入相应内容：

   - **名称**：设置云路由规格名称
   - **简介**：可选项，可留空不填
   - **CPU**：设置CPU个数，生产环境中建议个数设置为8以上
   - **内存**：设置内存大小，单位包括：M、G、T，生产环境中建议设置为8G以上
   - **镜像**：选择已添加的云路由镜像
   - **管理网络**：从网络列表中选择已创建的L3-管理网络
   - **公有网络**：从网络列表中选择已创建的L3-公有网络

   如图 *22:* 创建云路由规格所示，点击**确定**，创建云路由规格。

   图 22: 创建云路由规格

b) 将云路由规格共享给账户A和账户B。

在ZStack私有云主菜单，点击**网络资源** > **路由资源** > **云路由规格**按钮，在**云路由规格**页面点击云路由规格名称，点击**共享** > **操作** > **共享**按钮，选择账户A和账户B，点击**确定**完成共享。如图 *23:* 共享云路由规格所示：

图 23: 共享云路由规格

8. 在admin账户下创建VXLAN网络池，加载到相应集群，并共享给账户A和账户B。

   a) 在admin账户下创建VXLAN网络池。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **VXLAN Pool**，进入**VXLAN Pool**界面，点击**创建VXLAN Pool**，在弹出的**创建VXLAN Pool**界面，参考上述表 *8: VXLAN*网络池配置信息填写如下：

   - **名称**：设置VXLAN网络池名称
   - **简介**：可选项，可留空不填
   - **起始Vni**：可从1-16777214之间选择一个数字作为起始Vni
   - **结束Vni**：可从1-16777214之间选择一个数字作为结束Vni，需大于或等于起始Vni

     注:

     - VXLAN网络池最大可支持16M（16777216）个虚拟网络；
     - Vni范围支持1-16777214。
   - **集群**：可选项，可在创建VXLAN网络池时直接加载相应集群，也可在创建VXLAN网络池后再加载集群。

     注: 加载的集群内物理机需存在VTEP IP。
   - **VTEP CIDR**：设置VTEP相应的CIDR，例如192.168.28.1/24

     注:

     - 创建VXLAN网络池，加载集群，需设置相应的VTEP（VXLAN隧道端点），VTEP一般对应于集群内物理机的某一网卡IP地址，ZStack设置VTEP是基于相应的CIDR来配置；
     - VXLAN网络池加载到集群时，检查的是VTEP IP，与物理的二层设备无关。

如图 *24: 创建VXLAN网络池*所示，点击**确定**，创建VXLAN网络池。

图 24: 创建VXLAN网络池

b) 将VXLAN网络池共享给账户A和账户B。

在ZStack私有云主菜单，点击**网络资源** > **二层网络资源** > **VXLAN Pool**按钮，在**VXLAN Pool**页面点击VXLAN网络池名称，点击**共享** > **操作** > **共享**按钮，选择账户A和账户B，点击**确定**完成共享。如图 *25: 共享VXLAN网络池*所示：

图 25: 共享VXLAN网络池

9. 基于云路由规格在账户A和账户B分别创建一个VPC路由器。例如：VPC路由器-A和VPC路由器-B。

   在ZStack私有云主菜单，点击**网络资源** > **VPC** > **VPC路由器**，进入**VPC路由器**界面，点击**创建VPC路由器**，在弹出的**创建VPC路由器**界面，可参考以下示例输入相应内容：

   - **名称**：设置VPC云路由规格名称，例如：VPC路由器-A
   - **简介**：可选项，可留空不填
   - **云路由规格**：选择已创建的云路由规格
   - **DNS**：可选项，用于设置VPC路由器的DNS解析服务，默认指定223.5.5.5

   如图 *26: 创建VPC路由器-A*所示，点击**确定**按钮，完成VPC路由器-A创建。

   图 26: 创建VPC路由器-A

同理，在账户B，创建VPC路由器-B。

10.基于VXLAN网络池在账户A和账户B分别创建两个VXLAN网络（虚拟的二层网络），例如：L2-VXLAN-A1和L2-VXLAN-A2、L2-VXLAN-B1和L2-VXLAN-B2。

在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，可参考以下示例输入相应内容：

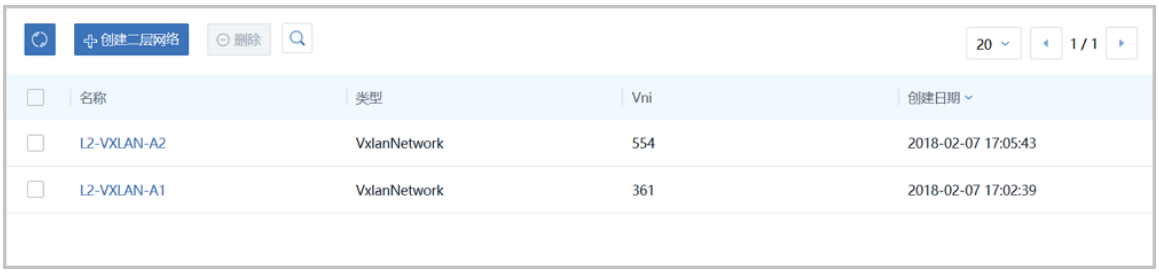
- **名称**：设置VXLAN网络名称，例如：L2-VXLAN-A1
- **简介**：可选项，可留空不填
- **类型**：选择VxlanNetwork
- **VXLAN网络池**：选择已创建的VXLAN网络池

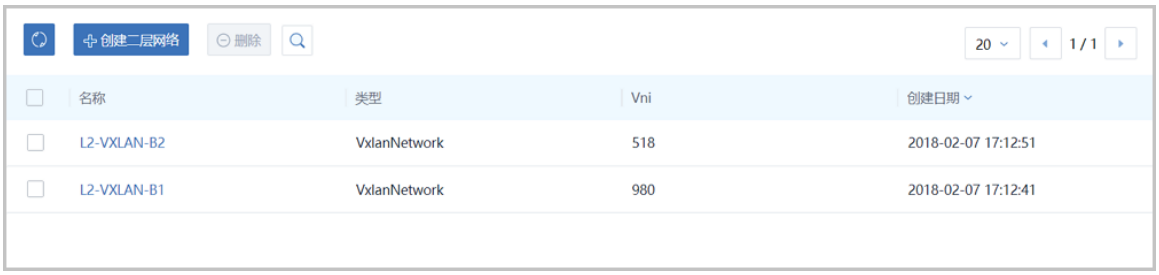
如图 *27: 创建L2-VXLAN-A1*所示，点击**确定**，创建L2-VXLAN-A1。

图 27: 创建L2-VXLAN-A1

同理，创建L2-VXLAN-A2、L2-VXLAN-B1和L2-VXLAN-B2。VXLAN网络，创建完成后如图 *28: VXLAN网络*所示：

图 28: VXLAN网络





11.使用四个VXLAN网络分别在各自账户创建VPC网路，例如：VPC网络-A1和VPC网络-A2、VPC网络-B1和VPC网络-B2。

在ZStack私有云界面，点击**网络资源** > **VPC** > **VPC网络**，进入**VPC网络**界面，点击**创建VPC网络**，在弹出的**创建VPC网络**界面，参考上述表 *9: VPC网络-A1*配置信息填写如下：

- **名称**：设置VPC网络名称，例如：VPC网络-A1
- **简介**：可选项，可留空不填
- **二层网络**：选择已创建的L2-VXLAN-A1
- **VPC路由器**：选择已创建的VPC路由器
- **关闭DHCP服务**：选择是否需要DHCP服务

  注:

  - 默认不勾选，表示启用DHCP服务，为云主机提供自动分配IP，此时DHCP IP支持自定义设置，也可由系统随机指定；
  - 勾选后，表示关闭DHCP服务，使用此网络的云主机将无法自动获取IP，需手动配置，此时DHCP IP不支持自定义设置，也不可由系统随机指定。
- **添加网络段**：选择CIDR
- **CIDR**：*192.168.21.0/24*
- **DHCP IP**：可选项，可按需设置DHCP IP

  注:

  - 若首次创建三层网络并启用DHCP服务，或对已启用DHCP服务的三层网络添加首个网络段，支持自定义设置DHCP IP；
  - 若三层网络已存在DHCP IP，添加网络段不允许自定义设置DHCP IP；
  - DHCP IP必须在添加的CIDR内，且未被占用；
  - 若留空不填，将由系统在添加的CIDR内随机指定；
  - CIDR内首个IP地址已被默认为网关，不可作为DHCP IP。
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *29: 创建VPC网络-A1*所示，点击**确定**，创建L3-VXLAN-云路由网络1。

图 29: 创建VPC网络-A1

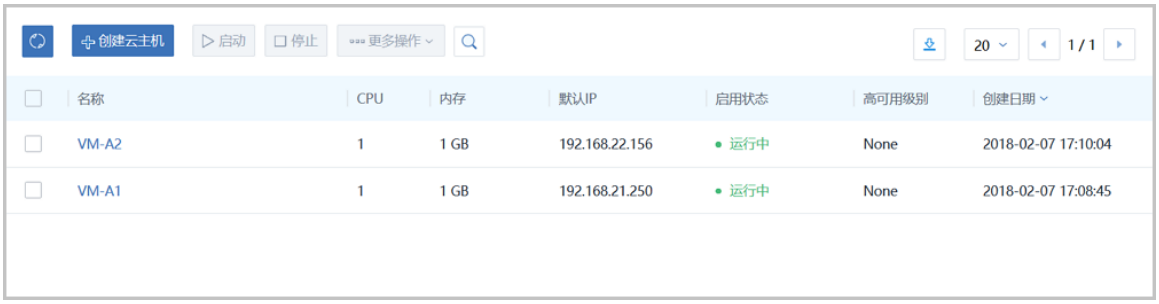
同理，创建VPC网络-A2、VPC网络-B1和VPC网络-B2，创建完成后如图 *30: VPC网络*所示：

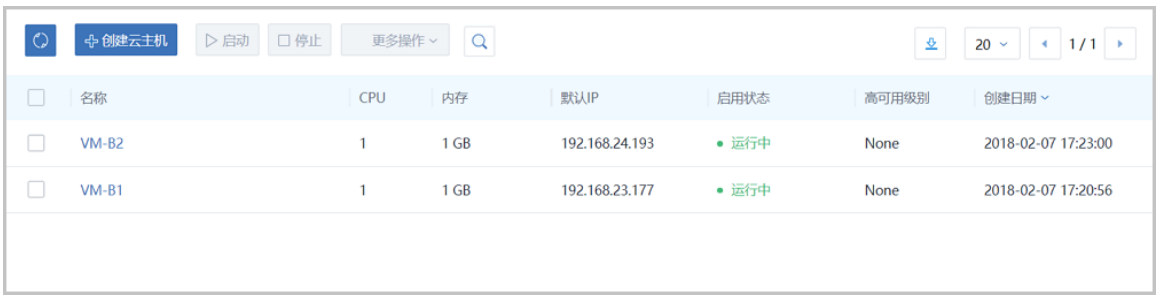
图 30: VPC网络

12.使用四个VPC网络分别在各自账户创建一个云主机，例如：VM-A1、VM-A2、VM-B1和VM-B2。

参考本教程基本部署章节的使用*VPC*网络创建云主机，使用四个VPC网络分别在各自账户创建一个云主机，VM-A1、VM-A2、VM-B1和VM-B2。创建的云主机如图 *31:* 创建云主机所示：

图 31: 创建云主机





13.验证四台云主机之间的连通性。

1. 登录VM-A1，用*ping*命令验证网络连通性：

   预期结果：

- ping baidu.com：可以成功
- ping VM-A2：可以成功
- ping VM-B1：会失败（两套VXLAN-VPC环境二层隔离）
- ping VM-B2：会失败（两套VXLAN-VPC环境二层隔离）

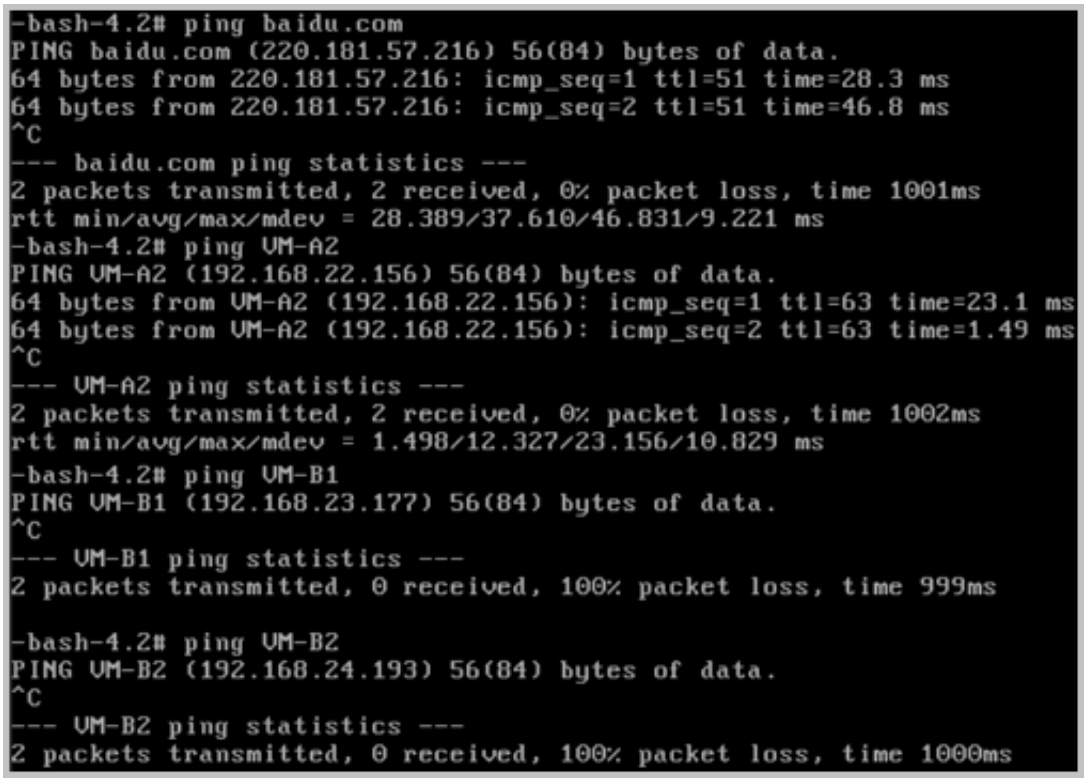
注:

在VM-A1系统中，手动添加其他VM的IP地址到*/etc/hosts*文件路径下。

```
[root@VM-web ~]# vim /etc/hosts
...
192.168.22.156 VM-A2
192.168.23.177 VM-B1
192.168.24.193 VM-B2
...
```

实际结果如图 *32: 验证VM-A1网络连通性*所示：

图 32: 验证VM-A1网络连通性



2. 同理，VM-A2的网络连通性和VM-A1相同。
3. 登录VM-B1，用*ping*命令验证网络连通性：

   预期结果：

- ping baidu.com：可以成功
- ping VM-A1：会失败（两套VXLAN-VPC环境二层隔离）
- ping VM-A2：会失败（两套VXLAN-VPC环境二层隔离）
- ping VM-B2：可以成功

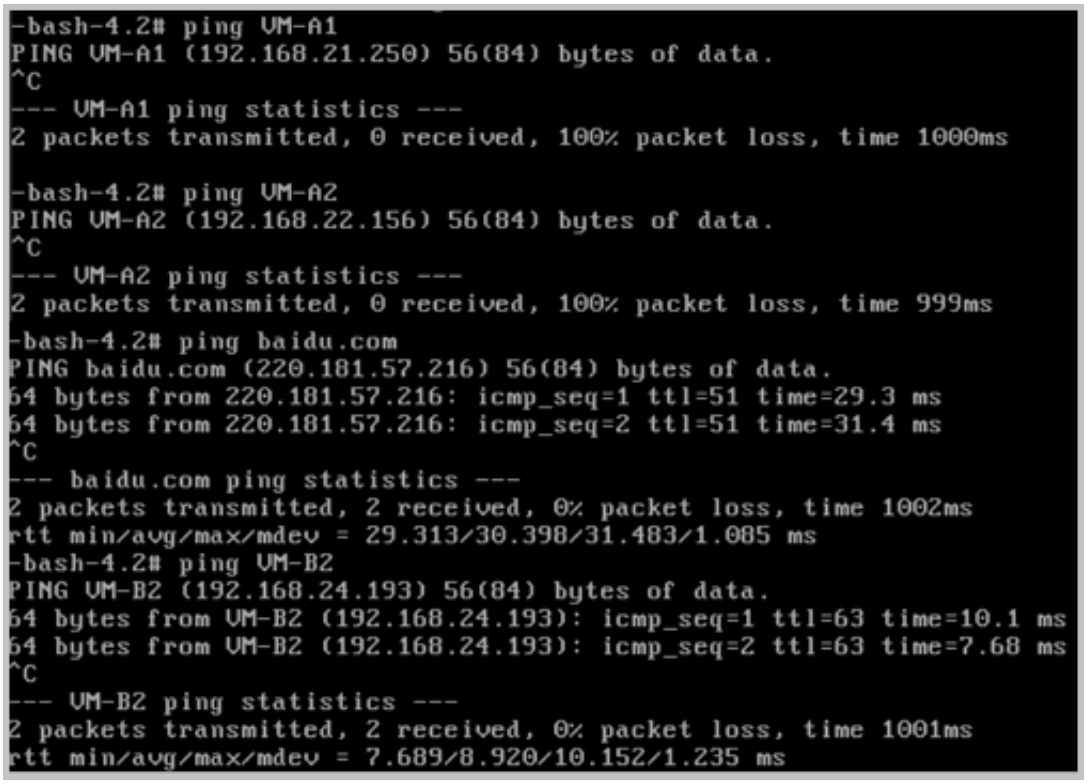
注:

在VM-B1系统中，手动添加其他VM的IP地址到*/etc/hosts*文件路径下。

```
[root@VM-web ~]# vim /etc/hosts
...
192.168.21.250 VM-A1
192.168.22.156 VM-A2
192.168.24.193 VM-B2
...
```

实际结果如图 *33:* 验证*VM-B2*网络连通性所示：

图 33: 验证VM-B2网络连通性



4. 同理，VM-B2的网络连通性和VM-B1相同。

14.从admin账户共享三层公有网络给账户A和账户B。

在ZStack私有云界面，点击**网络资源** > **三层网络** > **公有网络**，再**公有网络**界面点击三层公网名称，点击**共享** > **操作** > **共享**按钮，勾选账户A和账户B，点击**确定**按钮完成共享。如图 *34: 共享三层公网*所示：

图 34: 共享三层公网

15.通过配置路由表，可让二层隔离的云主机VM-A1和VM-B1互相访问。

a) 创建路由表。

在ZStack私有云界面，点击**网络资源** > **路由资源** > **路由表**，进入**路由表**界面，点击**创建路由表**，在弹出的**创建路由表**界面，可参考以下示例输入相应内容：

- **名称**：设置路由表名称
- **简介**：可选项，可留空不填
- **路由器**：选择VM-A1、VM-B1对应的云路由器

如图 *35: 创建路由表*所示：

图 35: 创建路由表

b) 添加两条自定义路由条目。

表 13: 自定义路由条目

	目标网段	**下一跳**
自定义路由条目1	VM-A1相应的云路由器的公网IP	VM-A1相应的云路由器的公网IP
自定义路由条目2	VM-B1相应的云路由器的公网IP	VM-B1相应的云路由器的公网IP

在**路由表**界面，点击已创建的路由表，进入路由表详情页，点击**路由条目**，进入**路由条目**界面，点击**操作** > **添加路由条目**，弹出**添加路由条目**界面，可依次添加上述两条自定义路由条目。如图 *36:* 添加路由表条目所示：

图 36: 添加路由表条目

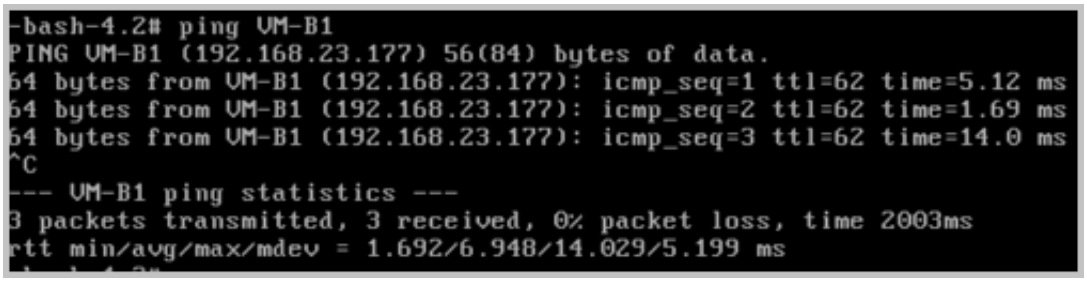
16.验证云主机VM-A1和VM-B1之间的连通性。

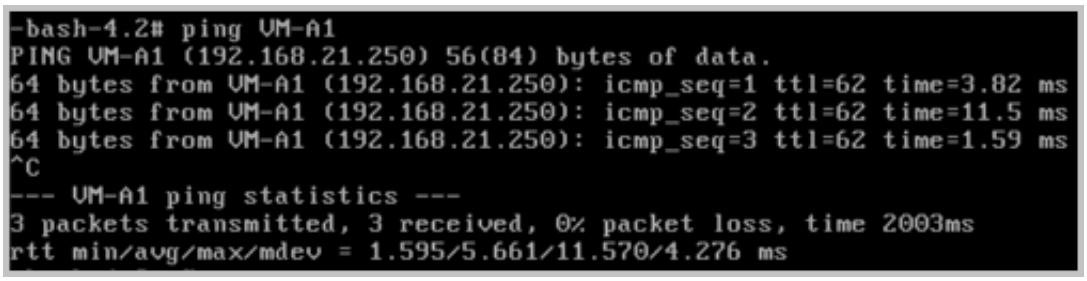
预期结果：

- 登录VM-A1，ping VM-B1：可以成功
- 登录VM-B1，ping VM-A2：可以成功

实际结果如图 *37: VM-A1和VM-B1互ping*所示：

图 37: VM-A1和VM-B1互ping





后续操作

至此，VPC网络多租户隔离部署实践介绍完毕。

4.2 多层Web服务器

背景信息

VPC下部署多层Web服务器的基本流程：

1. 在一个VPC下搭建三个VPC子网：Web网络、应用网络、数据库网络。

   注: 三个VPC子网的网络段不可重叠。

2. 基于三个VPC子网分别创建三台云主机：VM-web、VM-app、VM-database。
3. 验证三台云主机的网络连通性。

假定客户环境如下：

1. 公有网络

   表 14: 公有网络配置信息

公有网络	配置信息
网卡	em01
VLAN ID	非VLAN
IP地址段	*10.151.10.100~10.151.10.200*
子网掩码	*255.0.0.0*
网关	*10.0.0.1*

2. 管理网络

   表 15: 管理网络配置信息

管理网络	配置信息
网卡	em02
VLAN ID	非VLAN
IP地址段	*192.168.28.100~192.168.28.200*
子网掩码	*255.255.255.0*
网关	*192.168.28.1*

注:

- 出于安全和稳定性考虑，建议部署独立的管理网络，并与公有网络隔离。
- 此管理网络与ZStack私有云中的管理网络为相同概念（即：管理物理机、主存储、镜像服务器的网络），如果已创建可直接复用。

3. Web网络（VPC网络-1）

表 16: Web网络配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2017
IP CIDR	*192.168.10.0/24*

4. 应用网络（VPC网络-2）

表 17: 应用网络配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2020
IP CIDR	*192.168.20.0/24*

5. 数据库网络（VPC网络-3）

表 18: 数据库网络配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2050
IP CIDR	*192.168.50.0/24*
私有网络	配置信息

以下介绍VPC下部署多层Web服务器的实践步骤。

操作步骤

1. 在一个VPC下搭建三个VPC子网：Web网络、应用网络、数据库网络。详情可参考本教程基本部署章节。

注: 三个VPC子网的网络段不可重叠。

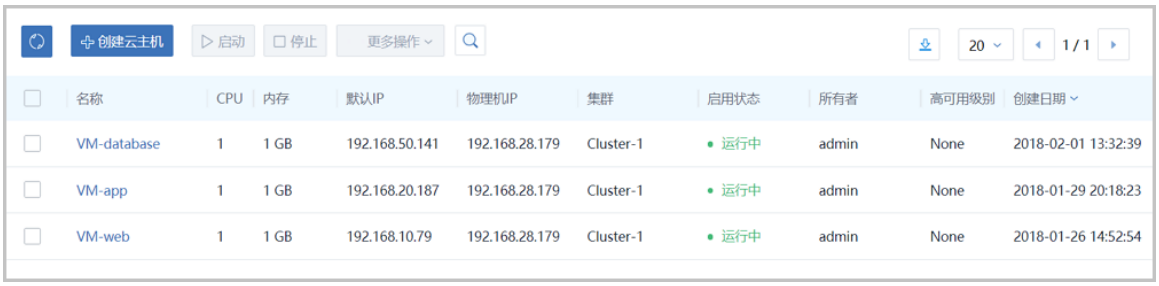
搭建的三个VPC子网如图 *38: 三个VPC子网*所示：

图 38: 三个VPC子网

2. 基于三个VPC子网分别创建三台云主机：VM-web、VM-app、VM-database。

   如图 *39: VM-web、VM-app、VM-database*所示：

   图 39: VM-web、VM-app、VM-database



3. 验证三台云主机的网络连通性。

   1. 登录VM-web，用*ping*命令验证网络连通性：

      预期结果：

      - ping baidu.com：可以成功
      - ping VM-app：可以成功
      - ping VM-database：可以成功

      注:

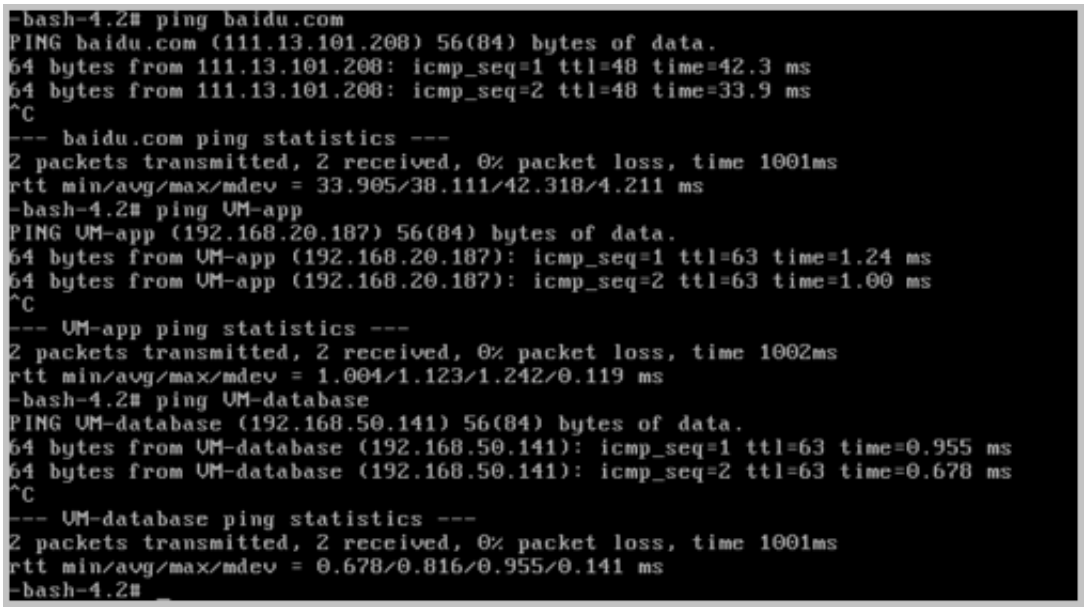
      在VM-web系统中，手动添加VM-app、VM-database的IP地址到*/etc/hosts*文件路径下。

      ```
      [root@VM-web ~]# vim /etc/hosts
      ```

```
...
192.168.20.187 VM-app
192.168.50.141 VM-database
...
```

实际结果如图 *40: 验证VM-web网络连通性*所示：

图 40: 验证VM-web网络连通性



2. 登录VM-app，用*ping*命令验证网络连通性：

   预期结果：

   - ping baidu.com：可以成功
   - ping VM-web：可以成功
   - ping VM-database：可以成功

   注:

   在VM-app系统中，手动添加VM-web、VM-database的IP地址到*/etc/hosts*文件路径下。

   ```
   [root@VM-app ~]# vim /etc/hosts
   ...
   192.168.10.79 VM-web
   192.168.50.141 VM-database
   ...
   ```

   实际结果如图 *41: 验证VM-app网络连通性*所示：

   图 41: 验证VM-app网络连通性

```
-bash-4.2# ping baidu.com
PING baidu.com (123.125.114.144) 56(84) bytes of data.
64 bytes from 123.125.114.144: icmp_seq=1 ttl=48 time=26.4 ms
64 bytes from 123.125.114.144: icmp_seq=2 ttl=48 time=26.5 ms
^C
--- baidu.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 26.461/26.497/26.534/0.166 ms
-bash-4.2# ping VM-web
PING VM-web (192.168.10.79) 56(84) bytes of data.
64 bytes from VM-web (192.168.10.79): icmp_seq=1 ttl=63 time=1.03 ms
64 bytes from VM-web (192.168.10.79): icmp_seq=2 ttl=63 time=1.05 ms
^C
--- VM-web ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.033/1.043/1.053/0.010 ms
-bash-4.2# ping VM-database
PING VM-database (192.168.50.141) 56(84) bytes of data.
64 bytes from VM-database (192.168.50.141): icmp_seq=1 ttl=63 time=0.886 ms
^C
--- VM-database ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.886/0.886/0.886/0.000 ms
-bash-4.2#
```

3. 登录VM-database，用*ping*命令验证网络连通性：

   预期结果：

   - ping baidu.com：可以成功
   - ping VM-app：可以成功
   - ping VM-web：可以成功

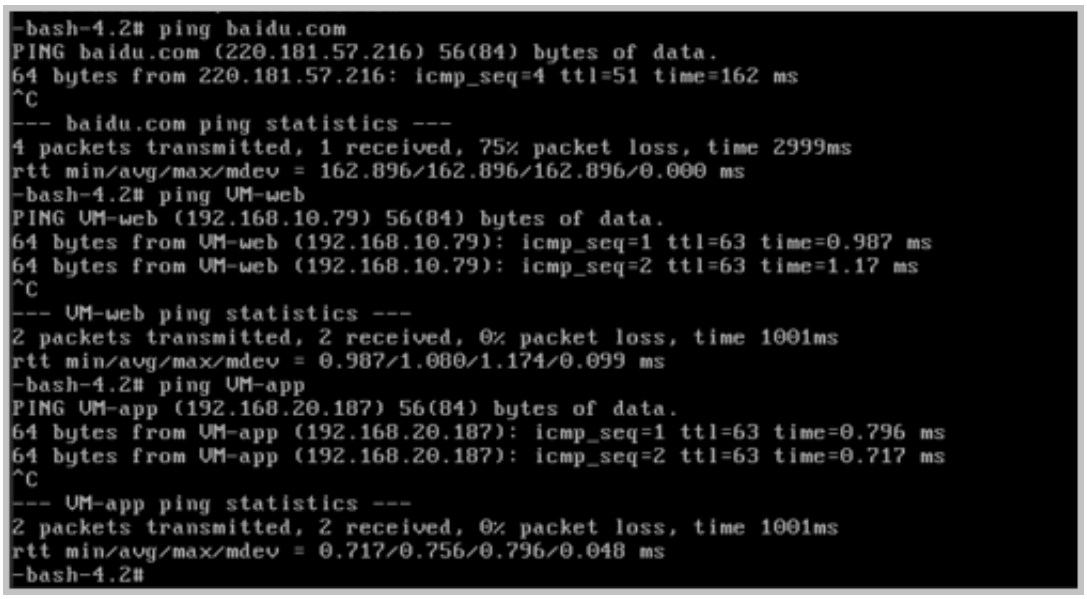
   注:

   在VM-database系统中，手动添加VM-app、VM-web的IP地址到*/etc/hosts*文件路径下。

   ```
   [root@VM-database ~]# vim /etc/hosts
   ...
   192.168.20.187 VM-app
   192.168.10.79 VM-web
   ...
   ```

实际结果如图 *42: 验证VM-database网络连通性*所示：

图 42: 验证VM-database网络连通性



后续操作

至此，多层Web服务器的部署实践介绍完毕。

4.3 安全组

前提条件

安全组：给云主机提供三层网络防火墙控制，控制TCP/UDP/ICMP等数据包进行有效过滤，对指定网络的指定云主机按照指定的安全规则进行有效控制。

- 扁平网络、云路由网络和VPC均支持安全组服务，安全组服务均由安全组网络服务模块提供，使用方法均相同：使用iptables进行云主机防火墙的安全控制。
- 安全组实际上是一个分布式防火墙；每次规则变化、加入/删除网卡都会导致多个云主机上的防火墙规则被更新。

安全组规则：

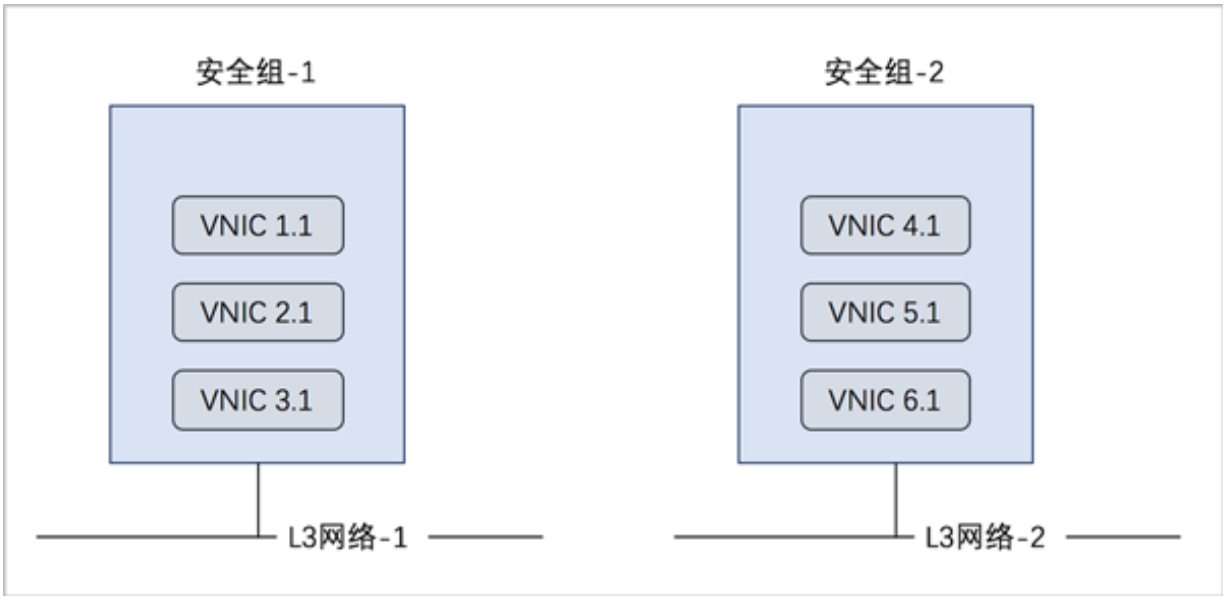
- 安全组规则按数据包的流向分为两种类型：
  - 入方向（Ingress）：代表数据包从外部进入云主机。
  - 出方向（Egress）：代表数据包从云主机往外部发出。
- 安全组规则对通信协议支持以下类型：
  - ALL：表示涵盖所有协议类型，此时不能指定端口。
  - TCP：支持1-65535端口。
  - UDP：支持1-65535端口。

  - ICMP：默认起始结束端口均为-1，表示支持全部的ICMP协议。
- 安全组规则支持对数据来源的限制，目前源可以设置为CIDR和安全组。
  - CIDR作为源：仅允许指定的CIDR才可通过
  - 安全组作为源：仅允许指定的安全组内的云主机才可通过

注: 如果两者都设置，只取两者交集。

如图 *43:* 安全组所示：

图 43: 安全组



背景信息

使用安全组的基本流程为：选择三层网络，设置相应的防火墙规则，选择指定的云主机加入规则中。

以下介绍VPC下安全组的使用方法，包括两个场景：

- VPC下仅有一个VPC网络（VPC子网）：安全组使用方法与云路由网络场景的安全组使用方法相同。
- VPC下有多个VPC子网：
  - 对两个VPC子网下的云主机设置入方向规则；
  - 对两个VPC子网下的云主机设置出方向规则。

操作步骤

1. 在一个VPC下搭建两个VPC子网，例如：VPC网络-1和VPC网络-2，使用VPC网络-1创建云主机VM-1，使用VPC网络-2创建云主机VM-2。详情可参考本教程基本部署章节。
2. 创建安全组。

   在ZStack私有云主菜单，点击**网络服务** > **安全组**，进入**安全组**界面，点击**创建安全组**，在弹出的**创建安全组**界面，可参考以下示例输入相应内容：

   - **名称**：设置安全组名称
   - **简介**：可选项，可留空不填
   - **网络**：选择已创建的VPC网络，例如：VPC网络-1
   - **规则**：可选项，用于设置相应的防火墙规则

     注: 创建安全组的时候可点击**规则**后面的**+**进行添加，也可后续添加，详见设置入方向规则和设置出方向规则。
   - **网卡**：可选项，选择网卡加入安全组

     注: 创建安全组的时候可点击**网络**后面的**+**进行添加，也可后续添加，详见添加网卡到安全组。

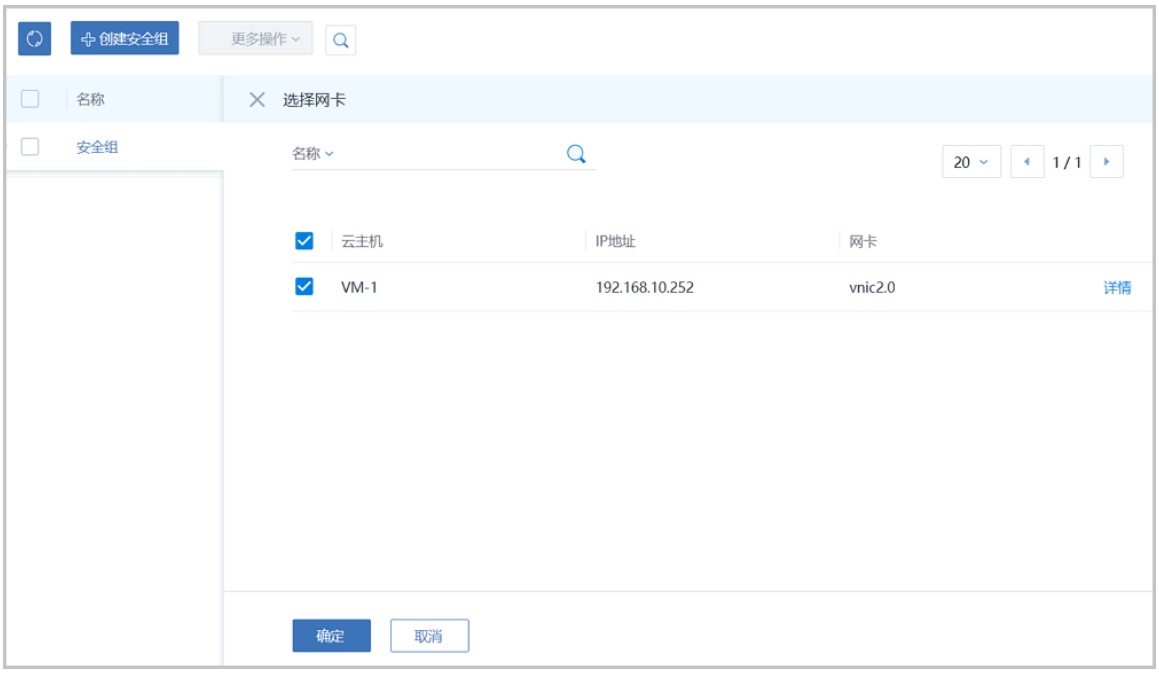
   如图 *44:* 创建安全组所示，点击**确定**完成安全组创建。

   图 44: 创建安全组

3. 添加网卡到安全组。

   在**安全组**界面，点击已创建的安全组名称，点击**云主机网卡**子页面的**操作 > 绑定云主机网卡**按钮，进入**选择网卡**界面，选择VM-1网卡，如图 *45:* 添加网卡所示，点击**确定**按钮完成网卡添加。

图 45: 添加网卡



4. 设置入方向规则并验证。

a) 设置入方向规则。

在**安全组**界面，点击已创建的安全组名称，点击**规则**子页面的**操作** > **添加规则**按钮，进入**设置规则**界面，可参考以下示例输入相应内容：

- **类型**：入方向
- **协议**：TCP
- **开始端口**：20
- **结束端口**：100
- **CIDR**：可选项，仅允许指定的CIDR才可通过，可留空不填
- **源安全组**：可选项，仅允许指定的安全组内的云主机才可通过，可留空不填

如图 *46:* 设置入方向规则所示，点击**确定**，完成入方向规则设置。

图 46: 设置入方向规则

b) 入方向规则验证。

此时VM-1只允许外部通过端口20~100访问。

1. 登录VM-2，使用*nc*命令通过20端口与VM-1建立通信连接，可成功通信。

注: 需将VM-1中原有的iptables规则清除，可使用命令iptables -F

如图 *47: VM-2在端口20向VM-1发送信息*和图 *48: VM-1在端口20接收信息成功*所示：

图 47: VM-2在端口20向VM-1发送信息

图 48: VM-1在端口20接收信息成功

2. 登录VM-2，使用*nc*命令通过10端口与VM-1建立通信，通信会失败。如图 *49: VM-2在端口10尝试连接VM-1失败*所示：

图 49: VM-2在端口10尝试连接VM-1失败

5. 设置出方向规则并验证。

a) 设置出方向规则。

在**安全组**界面，点击已创建的安全组名称，点击**规则**子页面的**操作** > **添加规则**按钮，进入**设置规则**界面，可参考以下示例输入相应内容：

- **类型**：出方向
- **协议**：TCP
- **开始端口**：200
- **结束端口**：1000
- **CIDR**：可选项，仅允许指定的CIDR才可通过，可留空不填
- **源安全组**：可选项，仅允许指定的安全组内的云主机才可通过，可留空不填

如图 *50:* 设置出方向规则所示，点击**确定**，完成入方向规则设置。

图 50: 设置出方向规则

b) 出方向规则验证。

此时云主机VM-1只允许通过端口200~1000访问外部地址。

1. 登录VM-1，使用*nc*命令通过200端口与VM-2建立通信，可成功通信。

注: 需将VM-2中原有的iptables规则清除，可使用命令iptables -F

如图 *51: VM-1在端口200向VM-2发送信息*和图 *52: VM-2在端口200接收信息成功*所示：

图 51: VM-1在端口200向VM-2发送信息

图 52: VM-2在端口200接收信息成功

2. 登录VM-1，使用*nc*命令通过10端口与VM-2建立通信，通信会失败。如图 *53: VM-1在端口10尝试连接VM-2失败*所示：

图 53: VM-1在端口10尝试连接VM-2失败

后续操作

至此，安全组的使用方法介绍完毕。

4.4 弹性IP

前提条件

弹性IP（EIP）：定义了通过公有网络访问内部私有网络的方法。

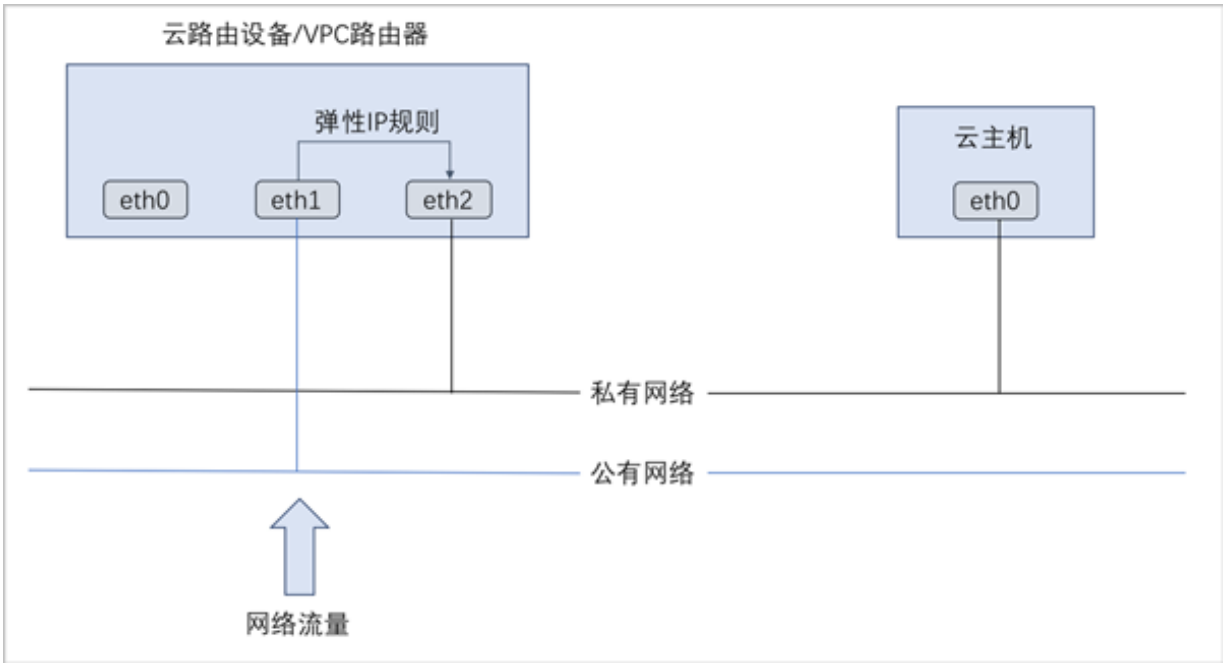
- 内部私有网络是隔离的网络空间，不能直接被外部网络访问。
- 弹性IP基于网络地址转换（NAT），将一个网络（通常是公有网络）的IP地址转换成另一个网络（通常是私有网络）的IP地址；通过弹性IP，可对公网的访问直接关联到内部私网的云主机IP。
- 弹性IP可动态绑定到一个云主机，或从一个云主机解绑。
- 云主机使用的扁平网络、云路由网络、VPC均可使用弹性IP服务：
  - 扁平网络：分布式EIP实现的弹性IP地址，可通过公有网络访问内部私有网络。
  - 云路由网络/VPC：使用云路由器/VPC路由器可通过公有网络访问云主机的私有网络。

- 内部私有网络是隔离的网络空间，不能直接被外部网络访问。
- 弹性IP基于网络地址转换（NAT），将一个网络（通常是公有网络）的IP地址转换成另一个网络（通常是私有网络）的IP地址；通过弹性IP，可对公网的访问直接关联到内部私网的云主机IP。
- 弹性IP可动态绑定到一个云主机，或从一个云主机解绑。
- 云主机使用的扁平网络、云路由网络、VPC均可使用弹性IP服务：
  - 扁平网络：分布式EIP实现的弹性IP地址，可通过公有网络访问内部私有网络。
  - 云路由网络/VPC：使用云路由器/VPC路由器可通过公有网络访问云主机的私有网络。

- 扁平网络：分布式EIP实现的弹性IP地址，可通过公有网络访问内部私有网络。
- 云路由网络/VPC：使用云路由器/VPC路由器可通过公有网络访问云主机的私有网络。

云路由网络/VPC下弹性IP的应用场景，如图 *54:* 云路由网络*/VPC*下弹性*IP*的应用场景所示：

图 54: 云路由网络/VPC下弹性IP的应用场景



背景信息

以下介绍VPC下弹性IP的使用方法，包括两个场景：

- 创建弹性IP并绑定一个云主机；
- 将弹性IP绑定其它云主机。

操作步骤

1. 在一个VPC下搭建两个VPC子网，例如：VPC网络-1和VPC网络-2，使用VPC网络-1创建云主机VM-1，使用VPC网络-2创建云主机VM-2。详情可参考本教程基本部署章节。
2. 创建弹性IP并绑定VM-1。

   a) 创建弹性IP。

   在ZStack私有云主菜单，点击**网络服务** > **弹性IP**，进入**弹性IP**界面，点击**创建弹性IP**，在弹出的**创建弹性IP**界面，可参考以下示例输入相应内容：

   - **名称**：设置弹性IP名称，例如EIP-1
   - **简介**：可选项，可留空不填
   - **选择虚拟IP**：通过虚拟IP提供弹性IP服务

     使用虚拟IP的方法有以下两种：

     - **新建虚拟IP**：

       如选择新建虚拟IP，需设置以下内容：

       - **网络**：选择提供虚拟IP的公有网络
       - **指定IP**：可选项，可指定虚拟IP；若留空不填，系统会自动分配虚拟IP

       如图 *55: 新建虚拟IP*所示：

       图 55: 新建虚拟IP

     - **已有虚拟IP**：

       如选择已有虚拟IP，需设置以下内容：

       - **虚拟IP**：选择已有的虚拟IP地址

如图 *56: 已有虚拟IP*所示：

图 56: 已有虚拟IP

如图 *57: 创建弹性IP*所示：

图 57: 创建弹性IP

b) 将EIP-1绑定VM-1。

云主机网卡可在创建弹性IP时直接添加，也可在创建弹性IP后再添加。

以创建弹性IP时直接绑定云主机网卡为例。在**创建弹性IP**界面点击**确定**后，会跳转到**绑定云主机网卡**界面，点击**云主机**栏里的加号按钮，弹出**选择云主机**界面，选择需要绑定的云主机，如：VM-1，点击**确定**。

如图 *58: 选择VM-1*和图 *59: 将EIP-1绑定VM-1*所示：

图 58: 选择VM-1

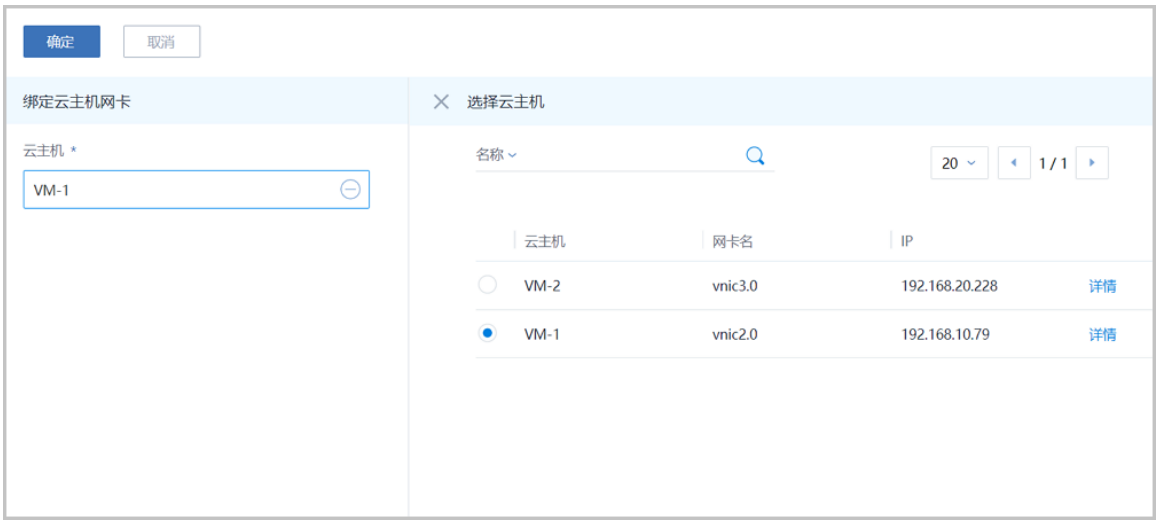


图 59: 将EIP-1绑定VM-1

c) 通过EIP-1登录VM-1。

使用某一可访问VPC网络公网网段的主机SSH登录EIP-1：*10.151.10.170*，也就是登录到私网IP为*192.168.10.79*的VM-1。

如所示：

图 60: 通过EIP-1登录VM-1

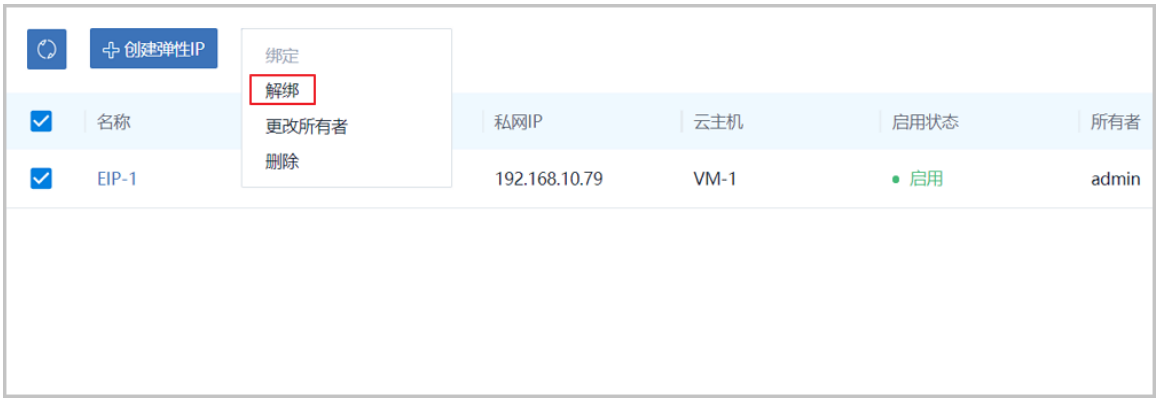
3. 将EIP-1绑定VM-2。

a) 将EIP-1从VM-1解绑。

在**弹性IP**界面，选择EIP-1，点击**更多操作** > **解绑**，弹出**解绑云主机**确认窗口，点击**确定**。

如图 *61: 将EIP-1从VM-1解绑*所示：

图 61: 将EIP-1从VM-1解绑



b) 将EIP-1绑定VM-2。

在**弹性IP**界面，选择EIP-1，点击**更多操作** > **绑定**，弹出**选择云主机**窗口，选择VM-2，点击**确定**。

如图 *62: 选择VM-2*和图 *63: 将EIP-1绑定VM-2*所示：

图 62: 选择VM-2

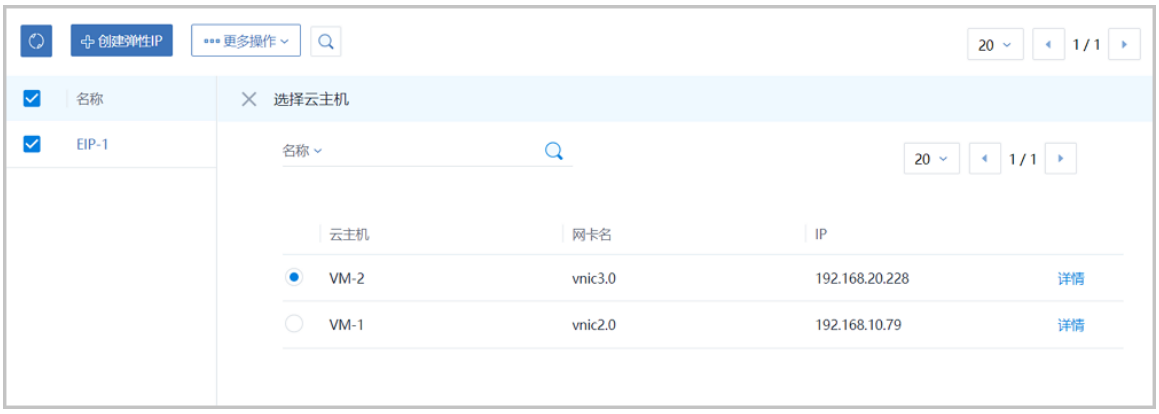


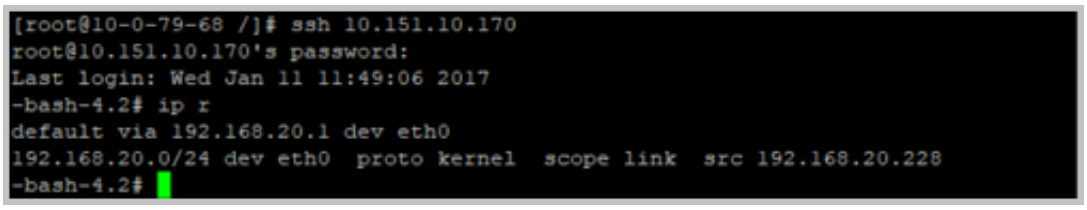
图 63: 将EIP-1绑定VM-2

c) 通过EIP-1登录VM-2。

再次SSH登录EIP-1：*10.151.10.170*，可发现此时登录到私网IP为*192.168.20.228*的VM-2。

如图 *64: 通过EIP-1登录VM-2*所示：

图 64: 通过EIP-1登录VM-2



后续操作

至此，弹性IP的使用方法介绍完毕。

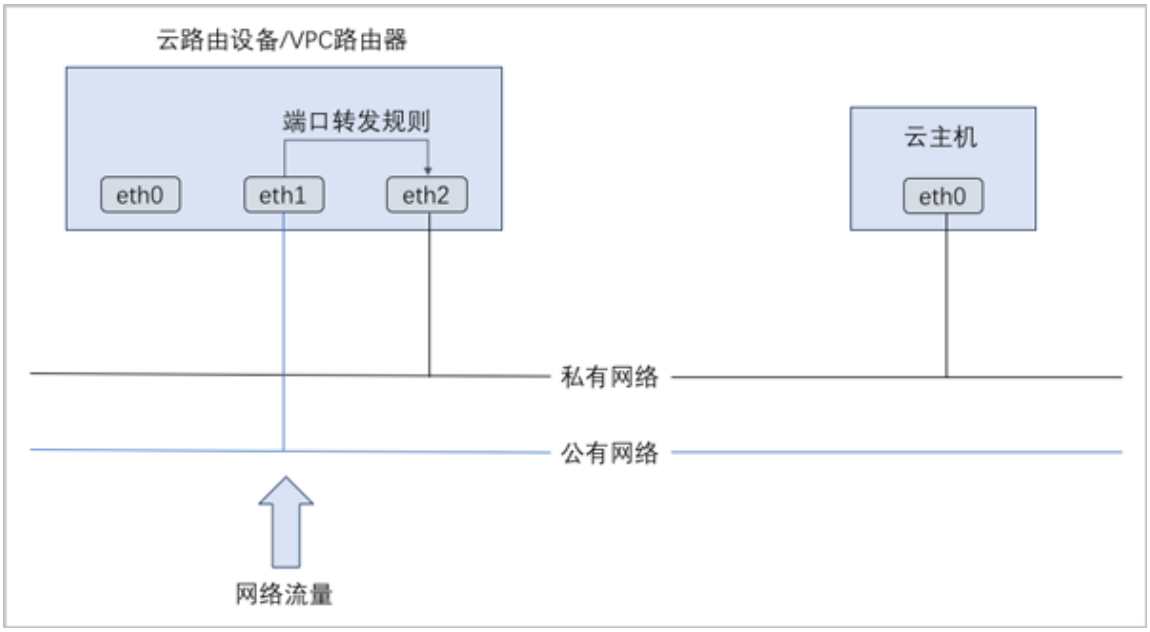
4.5 端口转发

前提条件

端口转发（PF）：基于云路由器/VPC路由器提供的三层转发服务，可将指定公有网络的IP地址端口流量转发到云主机对应协议的端口。在公网IP地址紧缺的情况下，通过端口转发可提供多个云主机对外服务，节省公网IP地址资源。

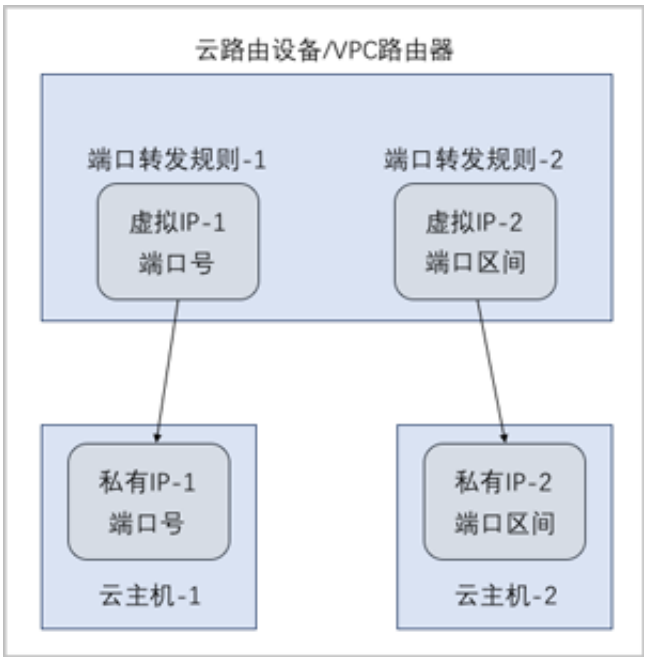
- 启用SNAT服务的私有网络中，云主机可访问外部网络但不能被外部网络所访问；使用端口转发规则，允许外部网络访问SNAT后面云主机的某些指定端口。
- 弹性端口转发规则可动态绑定到云主机，或从云主机解绑。
- 端口转发服务限于云路由器/VPC路由器提供。
  - 端口转发规则创建于云路由器/VPC路由器公有网络和云主机私有网络之间，如图 *65:* 端口转发所示：

图 65: 端口转发



- 通过虚拟IP提供端口转发服务。
  - 虚拟IP对应于公网IP地址资源池中的一个可用IP。
  - 端口转发使用虚拟IP有两种方法：新建虚拟IP、使用已有虚拟IP。
  - 端口转发指定端口映射有两种方法：单个端口到单个端口的映射、端口区间的映射。
  - 如图 *66:* 虚拟*IP*-端口转发所示：

图 66: 虚拟IP-端口转发



背景信息

以下介绍VPC下端口转发的使用方法，包括三个场景：

- 创建端口转发规则并绑定一个云主机；
- 将端口转发规则绑定其它云主机；
- 绑定同一虚拟IP的不同端口到不同云主机。

操作步骤

1. 在一个VPC下搭建两个VPC子网，例如：VPC网络-1和VPC网络-2，使用VPC网络-1创建云主机VM-1，使用VPC网络-2创建云主机VM-2。详情可参考本教程基本部署章节。
2. 创建端口转发规则并绑定VM-1。

   a) 创建端口转发规则。

   在ZStack私有云主菜单，点击**网络服务** > **端口转发**，进入**端口转发**界面，点击**创建端口转发**，在弹出的**创建端口转发**界面，可参考以下示例输入相应内容：

   - **名称**：设置端口转发规则名称，例如PF-1
   - **简介**：可选项，可留空不填
   - **选择虚拟IP**：通过虚拟IP提供端口转发服务，可选新建虚拟IP或已有虚拟IP方式添加
     - 新建虚拟IP方式，必须填写**网络**信息，可选填**指定IP**选项
     - 已有虚拟IP方式，必须填写**虚拟IP**信息

- **协议**：选择协议类型，包括：TCP、UDP
- **端口**：可选指定端口或端口区间方式添加，端口范围：1-65535
  - 指定端口方式，必须填写**源起始端口**和**云主机起始端口**，可选填**允许CIDR**
  - 端口区间方式，必须填写**源起始端口**和**源结束端口**，可选填**允许CIDR**

本场景下，使用指定端口方式（源起始端口：24，云主机起始端口：22）创建的端口转发规则PF-1如图 *67: 创建端口转发规则PF-1*所示，点击**确定**按钮完成端口转发创建。

图 67: 创建端口转发规则PF-1


确定
取消
创建端口转发
名称 *
PF-1
简介
选择虚拟IP
虚拟IP方法
新建虚拟IP
已有虚拟IP
虚拟IP *
vip-for-VPC路由器
协议 *
TCP
端口
指定端口
端口区间
源起始端口 *
24
源结束端口 *
24
云主机起始端口 *
22
云主机结束端口 *
22
允许CIDR:
192.168.1.0/24

b) 将PF-1绑定VM-1。

端口转发创建完成后会自动跳转到**绑定云主机网卡**界面，点击**云主机**栏里的加号按钮，弹出**选择云主机**界面，选择VM-1，点击**确定**。如图 *68: 选择VM-1*和图 *69: 将PF-1绑定VM-1*所示：

图 68: 选择VM-1

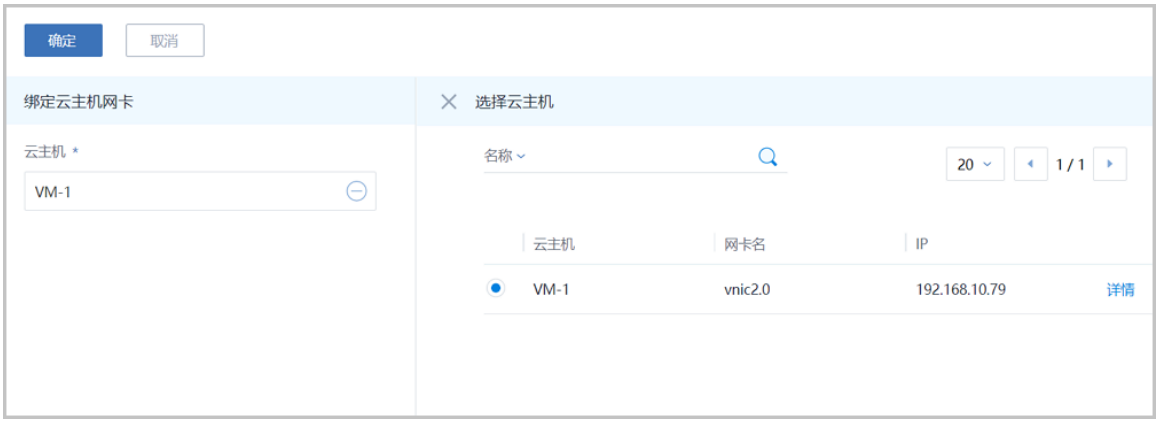


图 69: 将PF-1绑定VM-1

c) 通过PF-1登录VM-1。

使用某一可访问VPC网络公网网段的主机SSH登录公网IP：*10.151.10.174*的24端口，也就是登录到私网IP为*192.168.10.79*的VM-1的22端口。

如图 *70: 通过PF-1登录VM-1*所示：

图 70: 通过PF-1登录VM-1

```
login as: root
root@172.20.11.50's password:
Last login: Fri Jan 26 20:50:21 2018 from 172.31.253.12
[root@10-0-79-68 ~]# ssh 10.151.10.174 -p 24
root@10.151.10.174's password:
Last login: Fri Jan 26 12:51:39 2018 from 10.0.79.68
-bash-4.2# ip r
default via 192.168.10.1 dev eth0
192.168.10.0/24 dev eth0  proto kernel  scope link  src 192.168.10.79
-bash-4.2# lsof -i:22
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd      860 root    3u  IPv4  13120      0t0  TCP *:ssh (LISTEN)
sshd      860 root    4u  IPv6  13129      0t0  TCP *:ssh (LISTEN)
sshd    26134 root    3u  IPv4  42006      0t0  TCP zstack-test-image:ssh->10.0.
79.68:39284 (ESTABLISHED)
-bash-4.2#
```

3. 将PF-1绑定VM-2。

a) 将PF-1从VM-1解绑。

在**端口转发**界面，选择PF-1，点击**更多操作** > **解绑**，弹出**解绑云主机**确认窗口，点击**确定**。

如图 *71: 将PF-1从VM-1解绑*所示：

图 71: 将PF-1从VM-1解绑

b) 将PF-1绑定VM-2。

在**端口转发**界面，选择PF-1，点击**更多操作** > **绑定**，弹出**选择云主机**窗口，选择VM-2，点击**确定**。

如图 *72: 选择VM-2*和图 *73: 将PF-1绑定VM-2*所示：

图 72: 选择VM-2

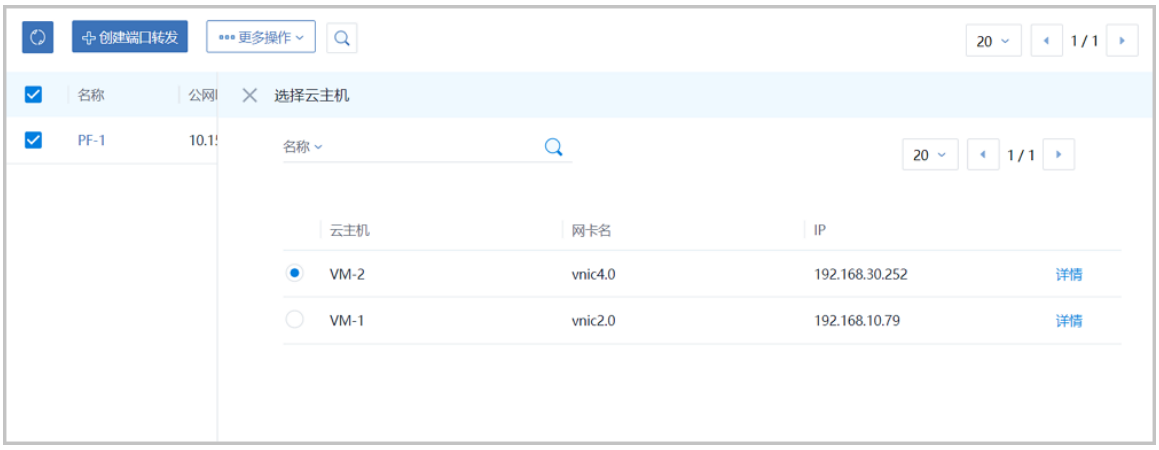


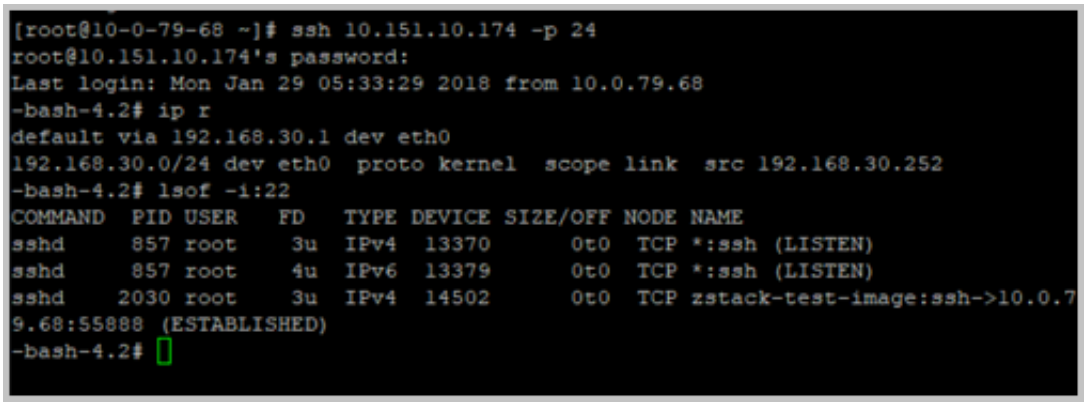
图 73: 将PF-1绑定VM-2

c) 通过PF-1登录VM-2。

再次SSH登录公网IP：*10.151.10.174*的24端口，可发现此时登录到私网IP为*192.168.30.252*的VM-2的22端口。

如图 *74: 通过PF-1登录VM-2*所示：

图 74: 通过PF-1登录VM-2



4. 绑定同一虚拟IP的不同端口到不同云主机。

a) 使用同一虚拟IP创建端口转发规则PF-2。

在ZStack私有云主菜单，点击**网络服务 > 端口转发**，进入**端口转发**界面，点击**创建端口转发**，在弹出的**创建端口转发**界面，可参考以下示例输入相应内容：

- **名称**：设置端口转发规则名称，例如PF-2
- **简介**：可选项，可留空不填
- **选择虚拟IP**：选择已有虚拟IP
- **协议**：选择协议类型，包括：TCP、UDP
- **端口**：选择端口区间方式，端口范围：1-65535
  - **源起始端口**：可从1-65535端口之间选择一个端口作为源起始端口，例如30
  - **源结束端口**：可从1-65535端口之间选择一个端口作为源结束端口，例如40
  - **云主机起始端口**：系统自动填写，默认与源起始端口一致
  - **云主机结束端口**：系统自动填写，默认与源结束端口一致
  - **允许CIDR**：可选项，仅允许指定的CIDR才可通过，可留空不填

如图 *75:* 创建端口转发规则*PF-2*所示，点击**确定**按钮完成端口转发创建。

图 75: 创建端口转发规则PF-2


确定
取消
创建端口转发
名称 *
PF-2
简介
选择虚拟IP
虚拟IP方法
新建虚拟IP
已有虚拟IP
虚拟IP *
vip-for-VPC路由器
协议 *
TCP
端口
指定端口
端口区间
源起始端口 *
30
源结束端口 *
40
云主机起始端口 *
30
云主机结束端口 *
40
允许CIDR:
192.168.1.0/24

b) 将PF-2绑定VM-1。

端口转发创建完成后会自动跳转到**绑定云主机网卡**界面，点击**云主机**栏里的加号按钮，弹出**选择云主机**界面，选择VM-1，点击**确定**。如图 *76: 选择VM-1*和图 *77: 将PF-2绑定VM-1*所示：

图 76: 选择VM-1

图 77: 将PF-2绑定VM-1

c) 可见，同一虚拟IP（*10.151.10.174*），通过不同的端口转发规则，绑定到不同云主机。

d) 通过PF-2向VM-1发送信息。

使用某一可访问VPC网络公网网段（*10.108.12.0~10.108.13.255*）的主机，通过*nc*命令向公网IP：*10.108.13.216*的5900~5910某端口发送信息，可在私网IP为*192.168.10.226*的VM-1相应端口接收信息。

例如，使用规则范围内的源端口5900发送信息，在VM-1的端口5900接收信息。

注： 需将VM-1中原先的iptables规则清除，可使用命令`iptables -F`

如图 *78: 在源端口30发送信息*和图 *79: 在VM-1的端口5900接收信息*所示：

图 78: 在源端口30发送信息

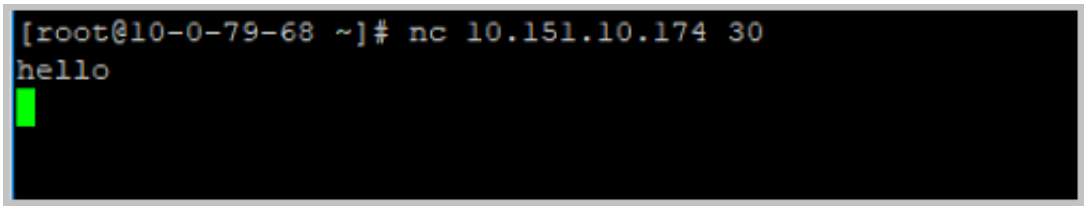


图 79: 在VM-1的端口5900接收信息

后续操作

至此，端口转发的使用方法介绍完毕。

4.6 负载均衡

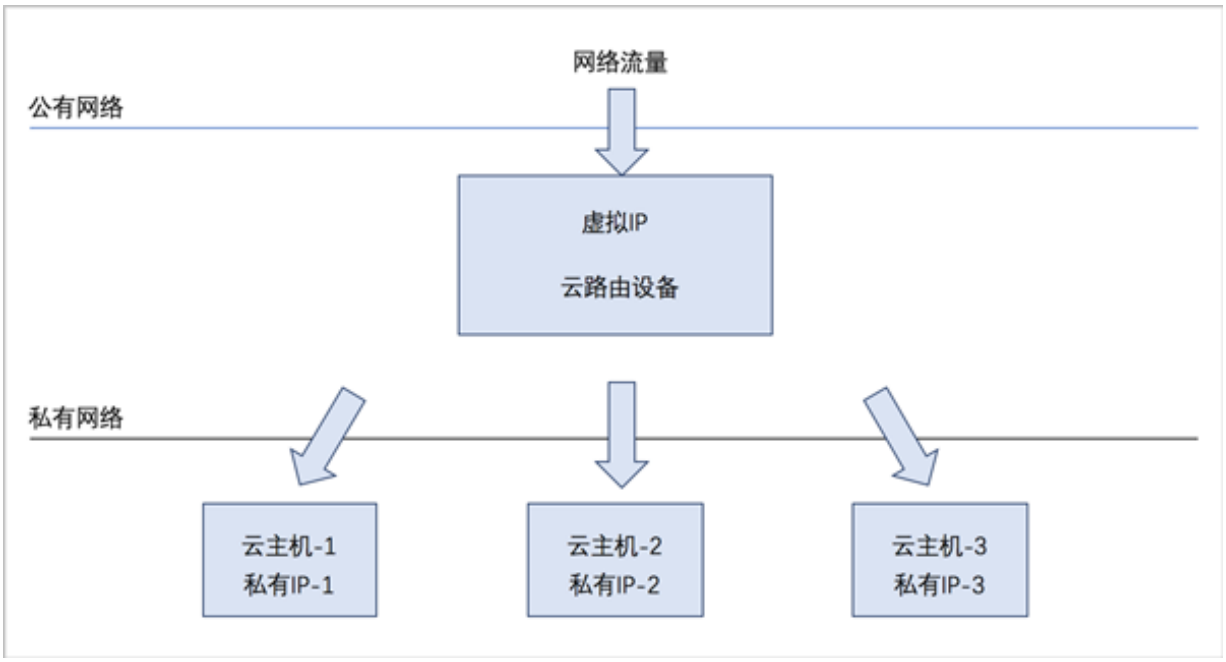
前提条件

负载均衡（LB）：将公网地址的访问流量分发到一组后端的云主机， 并支持自动检测并隔离不可用的云主机，从而提高业务的服务能力和可用性。

- 负载均衡自动把访问用户应用的流量分发到预先设置的多个后端云主机，以提供高并发高可靠的访问服务。
- 根据实际情况，动态调整负载均衡监听器中的云主机来调整服务能力，且不会影响业务的正常访问。
- 负载均衡监听器支持TCP/HTTP/HTTPS/UDP四种协议。
- 当监听协议为HTTPS，需绑定证书使用，支持上传证书和证书链。
- 负载均衡器支持灵活配置多种转发策略，实现高级转发控制功能。

如图 *80: 虚拟IP-负载均衡*所示，云路由网络/VPC下虚拟IP提供负载均衡服务。

图 80: 虚拟IP-负载均衡



背景信息

负载均衡的基本使用流程：

1. 创建负载均衡器。
2. 创建并添加监听器，指定公网端口到云主机端口的对应关系，设置规则及算法等。
3. 选择指定三层网络的云主机网卡绑定到监听器，使负载均衡器生效。

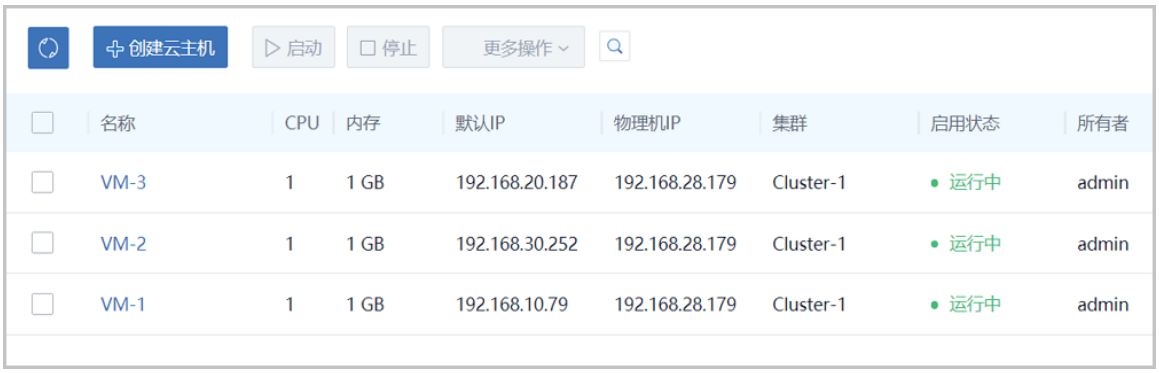
以下介绍VPC下负载均衡的使用方法，场景如下：

- 创建负载均衡器，添加一个监听器并绑定三台云主机，基于默认的轮询算法向三台云主机提供负载均衡服务。

操作步骤

1. 搭建三个VPC子网，例如：VPC网络-1、VPC网络-2和VPC网络-3，并分别创建云主机VM-1、VM-2和VM-3。详情可参考本教程基本部署章节。如图 *81: VM-1、VM-2、VM-3*所示：

   图 81: VM-1、VM-2、VM-3



2. 创建负载均衡器。

在ZStack私有云主菜单，点击**网络服务** > **负载均衡** > **负载均衡器**，进入**负载均衡器**界面，点击**创建负载均衡器**，在弹出的**创建负载均衡器**界面，可参考以下示例输入相应内容：

- **名称**：设置负载均衡器名称
- **简介**：可选项，可留空不填
- **选择虚拟IP**：通过虚拟IP提供负载均衡服务，可选新建虚拟IP或已有虚拟IP方式添加
  - 新建虚拟IP方式，必须填写**网络**信息，可选填**指定IP**选项
  - 已有虚拟IP方式，必须填写**虚拟IP**信息
- **监听器**：可选项，监听器可在创建负载均衡器时点击**创建监听器**按钮直接添加，也可在创建负载均衡器后再添加

  本场景以前者为例，详见添加监听器。

如创建负载均衡器所示：

图 82: 创建负载均衡器

3. 添加监听器。

   在**创建负载均衡器**界面，点击**创建监听器**按钮，弹出**添加监听器**界面，可参考以下示例输入相应内容：

   - **名称**：设置监听器名称

- **简介**：可选项，可留空不填
- **协议**：选择协议类型，包括：TCP、HTTP、HTTPS、UDP
  - TCP：支持1-65535端口
  - HTTP：支持1-65535端口
  - HTTPS：支持1-65535端口
  - UDP：支持1-65535端口
- **负载均衡端口**：可从1-65535端口之间选择一个端口作为负载均衡器公网端口
- **云主机端口**：可从1-65535端口之间选择一个端口作为云主机端口

  例如：公网端口选择80，云主机端口选择100，表示对负载均衡器公网IP的80端口访问会转发到云主机的100端口。

  如图 *83:* 添加监听器所示：

  图 83: 添加监听器

- **高级**：可对高级选项进行设置
  - **空闲连接超时**：没有数据传输时，触发负载均衡器终止服务器和客户端连接的超时时间，默认设置为60秒
  - **健康检查阈值**：对不健康的云主机，如果连续检查成功次数超过阈值，则认定其健康，默认设置为2次
  - **健康检查协议**：当监听协议为TCP/HTTP/HTTPS时，健康检查协议显示为TCP协议，当监听协议为UDP时，健康检查协议显示为UDP协议
  - **健康检查端口**：默认为default，表示与所选云主机端口一致，也可指定其它端口
  - **非健康检查阈值**：对云主机健康检查失败次数超过阈值，则认定其不健康，默认设置为2次
  - **健康检查间隔**：对云主机进行检查的时间间隔，默认设置为5秒

- **最大连接数量**：设置监听器最大的连接数量，默认设置为5000条，取值范围：1-100,000
- **负载均衡算法**：对网络包设定不同的路由规则，默认设置为**roundrobin**（轮询）

  支持的负载均衡算法包括：

  - **roundrobin**（轮询）

    通过轮询调度算法，将外部请求按顺序轮流分配到负载均衡规则指定的云主机中，它均等地对待每一台云主机，而不管其上实际的连接数和系统负载。

  - **leastconn**（最少连接）

    通过最少连接调度算法，将网络请求动态地调度到已建立的连接数最少的云主机上。如果集群中的服务器（云主机）具有相近的系统性能，采用最少连接调度算法可以较好地均衡负载。

  - **source**（源地址哈希）

    源地址哈希算法，根据请求的源IP地址，作为散列键（Hash Key）从静态分配的散列表找出对应的服务器，若该服务器可用且未超载，将请求发送到该服务器，否则返回空。

如图 *84:* 创建监听器-高级选项所示：

图 84: 创建监听器-高级选项

4. 绑定VM-1、VM-2、VM-3的云主机网卡到监听器。

   a) 进入绑定云主机网卡界面

   在ZStack私有云主菜单，点击**网络服务** > **负载均衡** > **监听器**按钮，进入**监听器**页面，选择一个监听器，点击**更多操作** > **绑定云主机网卡**，进入**绑定云主机网卡**界面。如图 *85:* 绑定云主机网卡所示：

   图 85: 绑定云主机网卡

b) 在弹出的**绑定云主机网卡**界面，可参考以下示例输入相应内容：

- **网络**：选择VPC路由器挂载的三层私有网络
- **云主机网卡**：选择网络对应的云主机

以VPC网络-3为例，如图 *86: 绑定VM-3网卡到监听器*所示，点击**确定**，绑定VM-3的云主机网卡到监听器。

图 86: 绑定VM-3网卡到监听器

重复此操作，绑定其他两个子网的网卡，绑定后如图 *87: 绑定云主机网卡到监听器*所示：

图 87: 绑定云主机网卡到监听器

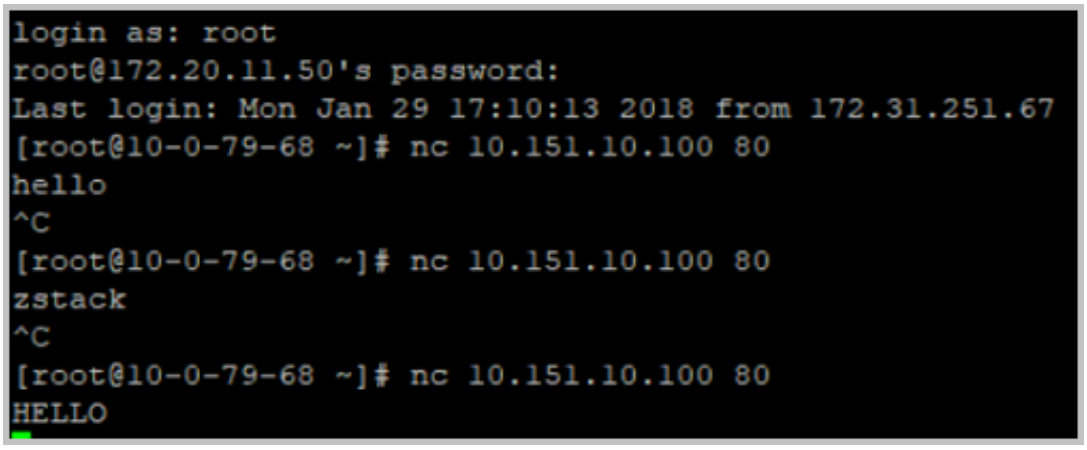
5. 负载均衡器以默认的轮询方式向三台云主机发送信息。

使用某一可访问VPC网络公网网段的主机，通过*nc*命令向负载均衡器公网IP：*10.151.10.100*的80端口发送信息，可在VM-1（私网IP：*192.168.10.76*）、VM-2（私网IP：*192.168.30.252*）、VM-3（私网IP：*192.168.20.187*）的100端口以默认的轮询方式接收信息。

注: 需将VM-1、VM-2、VM-3中原先的iptables规则清除，可使用命令`iptables -F`

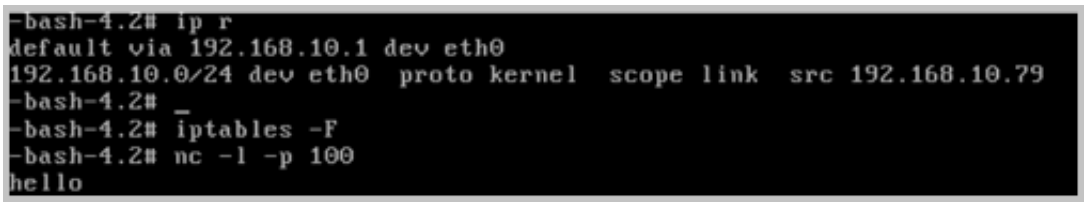
1. 向负载均衡器公网IP的80端口发送三条信息，如图 *88: 向负载均衡器公网IP的80端口发送三条信息*所示：

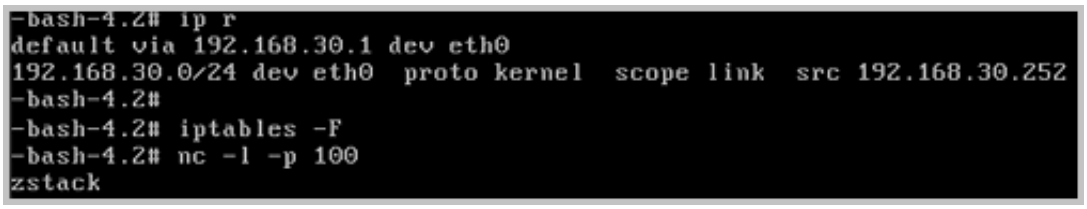
图 88: 向负载均衡器公网IP的80端口发送三条信息

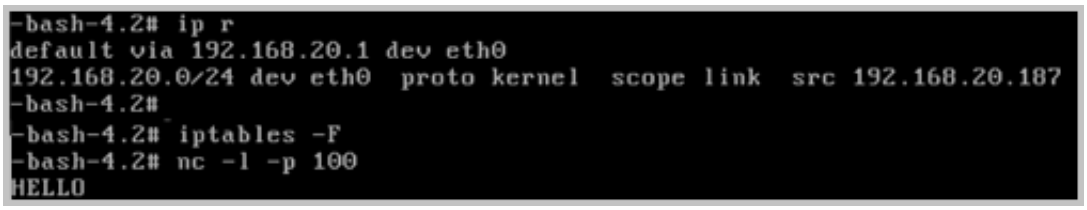


2. VM-1、VM-2、VM-3的100端口分别接收到一条信息，如图 *89: 三台云主机的100端口分别接收到一条信息*所示：

图 89: 三台云主机的100端口分别接收到一条信息







后续操作

至此，负载均衡的使用方法介绍完毕。

4.7 IPsec隧道

前提条件

IPsec隧道：透过对IP协议的分组加密和认证来保护IP协议的网络传输数据，实现站点到站点（site-to-site）的虚拟私有网络（VPN）连接。

VPC IPsec隧道的典型场景：

- 在两套隔离的ZStack私有云环境中，分别搭建两套VPC环境，在两套VPC环境中，分别创建两套VPC网络（VPC子网），两套VPC环境的子网间无法直接通信，使用IPsec隧道后，就可实现两套VPC环境的子网间互相通信。

背景信息

VPC IPsec隧道的使用流程：

1. 在第一套ZStack环境中，创建IPsec隧道，指定第一套VPC环境中的本地公网IP，并指定本地可用的一个或多个VPC子网，输入第二套VPC环境中的公网IP作为远端IP，并输入第二套VPC环境指定的一个或多个VPC子网作为远端网络；

2. 在第二套ZStack环境中，创建IPsec隧道，指定第二套VPC环境中的本地公网IP，并指定本地可用的一个或多个VPC子网，输入第一套VPC环境中的公网IP作为远端IP，并输入第一套VPC环境指定的一个或多个VPC子网作为远端网络。

注: 两套VPC环境中的所有私有网络段不可重叠。

假定客户环境如下：

- **第一套ZStack**：

  1. 公有网络

     表 19: 公有网络配置信息

公有网络	配置信息
网卡	em01
VLAN ID	非VLAN
IP地址段	*10.151.10.100~10.151.10.200*
子网掩码	*255.0.0.0*
网关	*10.0.0.1*

  2. 管理网络

     表 20: 管理网络配置信息

管理网络	配置信息
网卡	em02
VLAN ID	非VLAN
IP地址段	*192.168.28.100~192.168.28.200*
子网掩码	*255.255.255.0*
网关	*192.168.28.1*

     注:

     - 出于安全和稳定性考虑，建议部署独立的管理网络，并与公有网络隔离。
     - 此管理网络与ZStack私有云中的管理网络为相同概念（即：管理物理机、主存储、镜像服务器的网络），如果已创建可直接复用。

3. VPC网络-1

表 21: VPC网络-1配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2018
IP CIDR	*192.168.10.0/24*

4. VPC网络-2

表 22: VPC网络-2配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2020
IP CIDR	*192.168.20.0/24*

- **第二套ZStack**：

1. 公有网络

表 23: 公有网络配置信息

公有网络	配置信息
网卡	em01
VLAN ID	非VLAN
IP地址段	*10.151.20.100~10.151.20.200*
子网掩码	*255.0.0.0*
网关	*10.0.0.1*

2. 管理网络

表 24: 管理网络配置信息

管理网络	配置信息
网卡	em02

管理网络	配置信息
VLAN ID	非VLAN
IP地址段	*192.168.28.10~192.168.28.90*
子网掩码	*255.255.255.0*
网关	*192.168.28.1*

3. VPC网络-3

表 25: VPC网络-3配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2017
IP CIDR	*192.168.30.0/24*

4. VPC网络-4

表 26: VPC网络-4配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2030
IP CIDR	*192.168.40.0/24*

以下介绍搭建VPC IPsec隧道的实践步骤。

操作步骤

1. 在第一套ZStack中搭建VPC环境，并创建两套VPC网络（VPC子网），例如：VPC网络-1、VPC网络-2；使用VPC网络-1创建一台云主机VM-1，使用VPC网络-2创建一台云主机VM-2。详情可参考本教程基本部署章节。

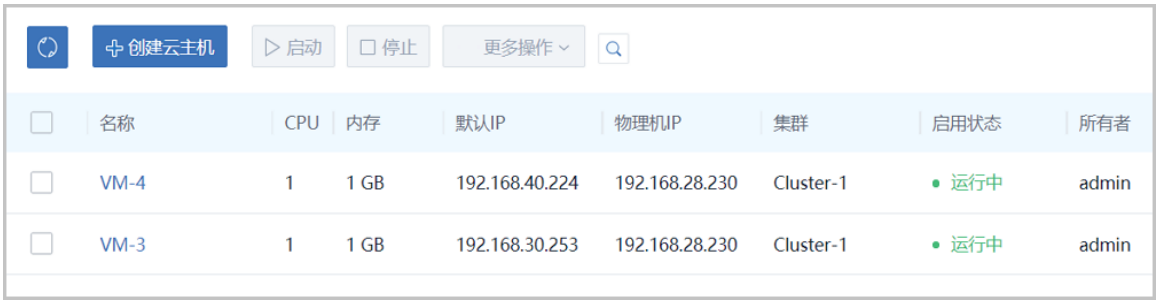
   创建的云主机如图 *90: VM-1、VM-2*所示：

图 90: VM-1、VM-2

2. 同理，在第二套ZStack中搭建VPC环境，并创建两套VPC网络（VPC子网），例如：VPC网络-3、VPC网络-4；使用VPC网络-3创建云主机VM-3，使用VPC网络-4创建云主机VM-4。

   创建的云主机如图 *91: VM-3、VM-4*所示：

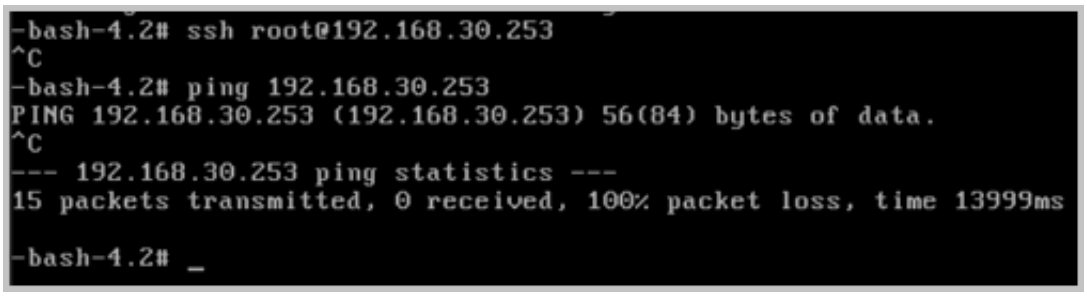
   图 91: VM-3、VM-4



3. 检测第一套VPC环境中的云主机VM-1、VM-2与第二套VPC环境中的云主机VM-3、VM-4的连通性。

   - 登录VM-1，尝试SSH默认的22端口远程登录VM-3失败，也不能ping通VM-3。
   - 如图 *92: VM-1尝试连通VM-3失败*所示：

     图 92: VM-1尝试连通VM-3失败



   - 登录VM-1，尝试连通VM-4失败。
   - 登录VM-2，尝试连通VM-3、VM-4失败。
   - 登录VM-3，尝试连通VM-1、VM-2失败。

- 登录VM-4，尝试连通VM-1、VM-2失败。

4. 在第一套ZStack中创建IPsec隧道。

a) 创建IPsec隧道-1。

在ZStack私有云主菜单，点击**网络服务** > **IPsec隧道**，进入**IPsec隧道**界面，点击**创建IPsec隧道**，在弹出的**创建IPsec隧道**界面，可参考以下示例输入相应内容：

- **名称**：设置IPsec隧道名称，例如IPsec隧道-1
- **简介**：可选项，可留空不填
- **选择虚拟IP**：通过虚拟IP提供IPsec服务

  使用虚拟IP的方法有以下两种：

  - **新建虚拟IP**：

    如选择新建虚拟IP，需设置以下内容：

    - **网络**：选择提供虚拟IP的公有网络
    - **指定IP**：可选项，可指定虚拟IP；若留空不填，系统会自动分配虚拟IP
  - **已有虚拟IP**：

    如选择已有虚拟IP，需设置以下内容：

    - **虚拟IP**：选择已有的虚拟IP地址

    注: VPC路由器提供的系统虚拟IP支持用于IPsec服务。
- **本地子网**：选择本地VPC路由器挂载的两个VPC子网，如果VPC路由器仅挂载一个VPC子网则会默认选中该VPC网络
- **远端网络IP**：填写远端VPC环境中用于IPsec服务的公网IP
- **远端网络CIDR**：填写远端VPC环境中指定的一个或多个VPC子网CIDR（多个VPC子网CIDR用","隔开）
- **认证密钥**：设置密钥，建议设置强度较高的密钥
- **高级选项**：可对高级选项进行设置，以下默认选项为可连通双边私网的选项
  - **认证模式**：psk（默认）
  - **工作模式**：tunnel（默认）
  - **IKE 验证算法**：sha1（默认）
  - **IKE 加密算法**：3des（默认）

- **IKE 完整前向保密**：2（默认）
- **传输安全协议**：esp（默认）
- **ESP 认证算法**：sha1（默认）
- **ESP 加密算法**：3des（默认）
- **完全正向保密(PFS)**：dh-group2（默认）

注:

- 如果客户场景设计ZStack私有云的VPC路由器与支持IPsec隧道的第三方设备对接，则需两端协商具体的高级配置信息。
- 创建IPsec隧道时，需根据远端网络设备IPsec配置内容，调整本地高级设置内容。

如图 *93: 创建IPsec隧道-1*所示，点击**确定**按钮，创建IPsec隧道。

图 93: 创建IPsec隧道-1


确定
取消
创建IPsec隧道
名称 *
IPsec隧道-1
简介
选择虚拟IP
虚拟IP方法
新建虚拟IP
已有虚拟IP
虚拟IP *
vip-for-VPC路由器
本地子网 *
VPC网络-1
VPC网络-2
远端网络IP *
10.151.20.192
远端网络CIDR *
192.168.30.0/24,192.168.40.0/24
认证密钥 *
test1234

IPsec隧道-1创建完成，如图 *94: IPsec隧道-1*所示：

图 94: IPsec隧道-1

5. 同理，在第二套ZStack中创建IPsec隧道。

   a) 创建IPsec隧道-2。

   如图 *95: 创建IPsec隧道-2*所示：

   图 95: 创建IPsec隧道-2


确定
取消
创建IPsec隧道
名称 *
IPsec隧道-2
简介
选择虚拟IP
虚拟IP方法
新建虚拟IP
已有虚拟IP
虚拟IP *
vip-for-VPC路由器
本地子网 *
VPC网络-4
VPC网络-3
远端网络IP *
10.151.10.174
远端网络CIDR *
192.168.10.0/24,192.168.20.0/24
认证密钥 *
test1234

b) IPsec隧道-2创建完成。

如图 *96: IPsec隧道-2*所示：

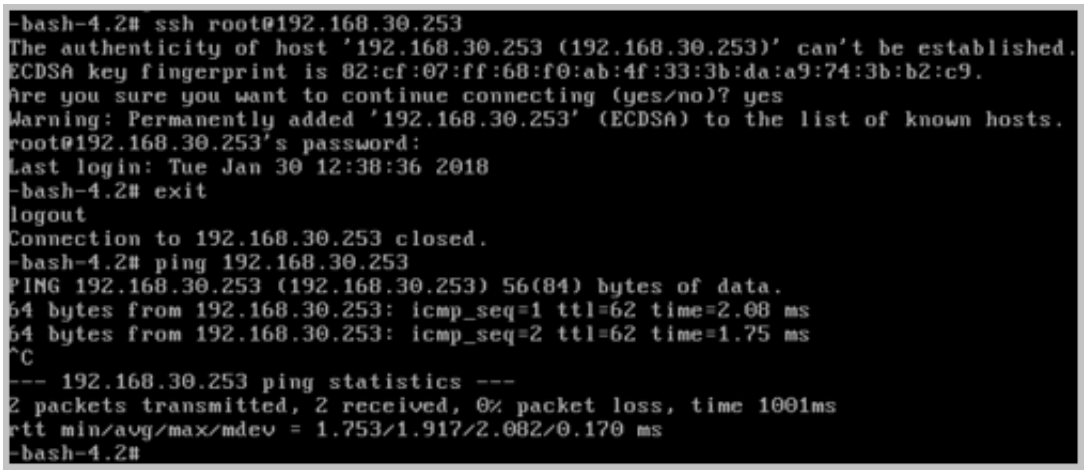
图 96: IPsec隧道-2

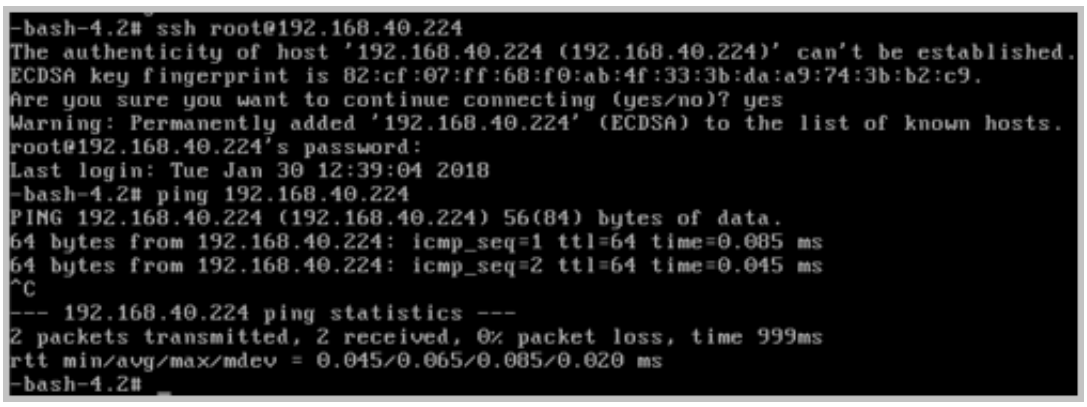
6. 检测第一套VPC环境中的云主机VM-1、VM-2与第二套VPC环境中的云主机VM-3、VM-4的连通性。

   - 登录VM-1，可通过SSH默认的22端口远程登录VM-3、VM-4，以及ping通VM-3、VM-4。

     如图 *97: VM-1成功连通VM-3、VM-4*所示：

     图 97: VM-1成功连通VM-3、VM-4





- 登录VM-2，可通过SSH默认的22端口远程登录VM-3、VM-4，以及ping通VM-3、VM-4。
- 登录VM-3，可通过SSH默认的22端口远程登录VM-1、VM-2，以及ping通VM-1、VM-2。

  如图 *98: VM-3成功连通VM-1、VM-2*所示：

  图 98: VM-3成功连通VM-1、VM-2

```
-bash-4.2# ssh root@192.168.10.79
The authenticity of host '192.168.10.79 (192.168.10.79)' can't be established.
ECDSA key fingerprint is 82:cf:07:ff:68:f0:ab:4f:33:3b:da:a9:74:3b:b2:c9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.79' (ECDSA) to the list of known hosts.
root@192.168.10.79's password:
Last login: Tue Jan 30 08:17:16 2018
-bash-4.2# exit
logout
Connection to 192.168.10.79 closed.
-bash-4.2# ping 192.168.10.79
PING 192.168.10.79 (192.168.10.79) 56(84) bytes of data.
64 bytes from 192.168.10.79: icmp_seq=1 ttl=62 time=1.67 ms
64 bytes from 192.168.10.79: icmp_seq=2 ttl=62 time=1.68 ms
^C
--- 192.168.10.79 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.677/1.682/1.688/0.041 ms
-bash-4.2#
```

```
-bash-4.2# ssh root@192.168.20.187
The authenticity of host '192.168.20.187 (192.168.20.187)' can't be established.
ECDSA key fingerprint is 82:cf:07:ff:68:f0:ab:4f:33:3b:da:a9:74:3b:b2:c9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.20.187' (ECDSA) to the list of known hosts.
root@192.168.20.187's password:
Permission denied, please try again.
root@192.168.20.187's password:
Last failed login: Tue Jan 30 12:55:36 UTC 2018 from 192.168.30.253 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Tue Jan 30 12:40:04 2018 from 192.168.10.79
-bash-4.2# exit
logout
Connection to 192.168.20.187 closed.
-bash-4.2# ping 192.168.20.187
PING 192.168.20.187 (192.168.20.187) 56(84) bytes of data.
64 bytes from 192.168.20.187: icmp_seq=1 ttl=62 time=2.26 ms
64 bytes from 192.168.20.187: icmp_seq=2 ttl=62 time=1.61 ms
^C
--- 192.168.20.187 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.612/1.939/2.266/0.327 ms
-bash-4.2#
```

- 登录VM-4，可通过SSH默认的22端口远程登录VM-1、VM-2，以及ping通VM1、VM-2。

后续操作

至此，VPC IPsec隧道的使用方法介绍完毕。

术语表

区域（Zone）

ZStack中最大的一个资源定义，包括集群、二层网络、主存储等资源。

集群（Cluster）

一个集群是类似物理主机（Host）组成的逻辑组。在同一个集群中的物理主机必须安装相同的操作系统（虚拟机管理程序，Hypervisor），拥有相同的二层网络连接，可以访问相同的主存储。在实际的数据中心，一个集群通常对应一个机架（Rack）。

管理节点（Management Node）

安装系统的物理主机，提供UI管理、云平台部署功能。

计算节点（Compute Node）

也称之为物理主机（或物理机），为云主机实例提供计算、网络、存储等资源的物理主机。

主存储（Primary Storage）

用于存储云主机磁盘文件的存储服务器。支持本地存储、NFS、 Ceph、、Shared Mount Point等类型。

镜像服务器（Backup Storage）

也称之为备份存储服务器，主要用于保存镜像模板文件。建议单独部署镜像服务器。

镜像仓库（Image Store）

镜像服务器的一种类型，可以为正在运行的云主机快速创建镜像，高效管理云主机镜像的版本变迁以及发布，实现快速上传、下载镜像，镜像快照，以及导出镜像的操作。

云主机（VM Instance）

运行在物理机上的虚拟机实例，具有独立的IP地址，可以访问公共网络，运行应用服务。

镜像（Image）

云主机或云盘使用的镜像模板文件，镜像模板包括系统云盘镜像和数据云盘镜像。

云盘（Volume）

云主机的数据盘，给云主机提供额外的存储空间，共享云盘可挂载到一个或多个云主机共同使用。

计算规格（Instance Offering）

启动云主机涉及到的CPU数量、内存、网络设置等规格定义。

云盘规格（Disk Offering）

创建云盘容量大小的规格定义。

二层网络（L2 Network）

二层网络对应于一个二层广播域，进行二层相关的隔离。一般用物理网络的设备名称标识。

三层网络（L3 Network）

云主机使用的网络配置，包括IP地址范围、网关、DNS等。

公有网络（Public Network）

由因特网信息中心分配的公有IP地址或者可以连接到外部互联网的IP地址。

私有网络（Private Network）

云主机连接和使用的内部网络。

L2NoVlanNetwork

物理主机的网络连接不采用Vlan设置。

L2VlanNetwork

物理主机节点的网络连接采用Vlan设置，Vlan需要在交换机端提前进行设置。

VXLAN网络池（VXLAN Network Pool）

VXLAN网络中的 Underlay 网络，一个 VXLAN 网络池可以创建多个 VXLAN Overlay 网络（即 VXLAN 网络），这些 Overlay 网络运行在同一组 Underlay 网络设施上。

VXLAN网络（VXLAN）

使用 VXLAN 协议封装的二层网络，单个 VXLAN 网络需从属于一个大的 VXLAN 网络池，不同 VXLAN 网络间相互二层隔离。

云路由（vRouter）

云路由通过定制的Linux云主机来实现的多种网络服务。

安全组（Security Group）

针对云主机进行第三层网络的防火墙控制，对IP地址、网络包类型或网络包流向等可以设置不同的安全规则。

弹性IP（EIP）

公有网络接入到私有网络的IP地址。

快照（Snapshot）

某一个时间点上某一个磁盘的数据备份。包括自动快照和手动快照两种类型。